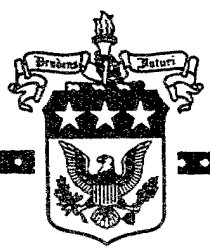
STRATEGY RESEARCH PROJECT

FORCE PROTECTION IN LARGE UNIT OPERATIONS

BY

DOUGLAS A. DARLING
Department of the Army

USAWC CLASS OF 2002



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

FORCE PROTECTION IN LARGE UNIT OPERATIONS

by

Douglas A. Darling
Department of the Army Civilian

COL John Bonin
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Mr. Douglas A. Darling

TITLE: Force Protection in Large Unit Operations

FORMAT: Strategy Research Project

DATE: 13 March 2002 PAGES: 75 CLASSIFICATION: Unclassified

This research project provides a draft force-protection chapter for use in a future Army field manual addressing large unit operations. The theater-strategic and operational level force protection tasks found in CJCSM 3500.04B, *Universal Joint Task List*, provide the basic structure of this draft chapter. Large unit operations are operations undertaken by units and organizations operating at the operational and theater strategic levels. The Army echelons that normally conduct large unit operations are corps or numbered army headquarters operating as the Army Force (ARFOR), joint force land component command (JFLCC), or joint task force headquarters. The Army service component command assigned to each commander of a combatant command also operates at the operational and theater strategic levels. If at some time in the future a peer competitor emerges, the U.S. Army could chose to resource one or more army group headquarters as part of a substantial reconstitution effort. In this unlikely event, the Army group headquarters will conduct operations at the operational and theater strategic level and its subordinate corps and numbered armies will conduct tactical operations. This research project takes as a given the theater level command and control structure documented in joint publications and the current draft FM 3-93 (100-7), *The Army in Theater Operations,* since it is only one chapter of a much longer field manual.

TABLE OF CONTENTS

PREFACE

Doctrine provides a common philosophy to those military organizations affected by it. It defines the common language that military professionals use to provide and understand the commander's intent and ensure unity of effort. This research project provides a draft doctrinal force protection chapter for use in a future Army large unit operations field manual. Large unit operations are operations undertaken by units and organizations operating at the operational and theater strategic levels. The Army echelons that normally conduct large unit operations are corps or numbered army headquarters operating as the Army Force (ARFOR), joint force land component command (JFLCC), or joint task force headquarters. The Army service component command assigned to each commander of a combatant command also operates at the operational and theater strategic levels. If at some time in the future a peer competitor emerges, the U.S. Army could choose to resource one or more army group headquarters as part of a substantial reconstitution effort. In this event, the Army group headquarters would conduct operations at the operational and theater strategic level and its subordinate corps and numbered armies will conduct tactical operations.

This conceptual large unit operations manual consists of eleven chapters. Chapter 1 would address theater organization and Army forces. Chapters 2 through 5 would address Army operational and theater-strategic participation in offensive, defensive, stability, and support operations. Chapters 6 through 11 would address the six operational level tasks defined in CJCSM 3500.04B, *Universal Joint Task List* (UJTL).

This research project would be Chapter 11 of this conceptual manual. The five components of force protection defined in FM 3-0 (100-5), *Operations*, provide the basic structure of this research project. The research project takes as a given the theater level structure documented in joint publications and the current draft FM 3-93 (100-7), *The Army in Theater Operations,* since it is only one chapter of a much longer field manual.

This draft chapter does not address some activities associated with the JP 1-02 definition of force protection because CJCSM 3500.04B, *Universal Joint Task List*, groups them with other related theater strategic and operational level tasks. These activities include—

- Individual health and welfare activities.
- Dispersion and mobility actions.
- Offensive counter air activities.
- Defensive IO actions comprising actions taken to maintain the integrity of friendly information despite adversary offensive IO.

The reader cannot read this draft chapter in isolation. To understand it, he must understand the art of operations at the theater-strategic and operational levels, principles of war, the Army's core competencies and the links between them. JP 3-0, *Doctrine for Joint Operations*, and FM 3-0 (100-5), *Operations*, describe those links. In an attempt to reduce unnecessary duplication, this draft chapter makes extensive references to other joint publications (JPs) and field manuals (FMs). Reviewing those references will aid in understanding this chapter.

I want to thank my long-suffering wife and family for their unlimited support during my year at the Army War College. My sons' abilities to function as productive members of the Leavenworth community—at school, at work, in extra-curricular activities, socially, and at church—while I was a thousand miles away speaks well for how their mother raised them. I am proud of them. I also want to thank the legion of Army NCOs with whom I have worked over the last thirty years, starting with my first platoon sergeant, SGT Tom Derry, for all that they have given to me. I hope that in some fashion, all the staff actions that I worked over my 18 years as a TRADOC staff officer have, in some fashion, helped pay their wisdom and knowledge forward to future generations of Army professionals.

Unless otherwise stated, masculine nouns or pronouns do not refer exclusively to men.

Bold text in this document indicates an official Joint or Army definition.

With the publication of Field Manuals 1 (100-1) and 3-0 (100-5) on 14 June 2001 the Army adopted the joint publication numbering system for its field manuals. This SRP uses the new number for each field manual first, followed by the old number—when it exists—to assist the reader in understanding what manual was referenced.

LIST OF ILLUSTRATIONS

LIST OF TABLES

FORCE PROTECTION IN LARGE UNIT OPERATIONS

Army officers do not understand operational force protection. There are two main reasons why this situation exists. First, the vast majority of the officers in the US Army do not understand the operational art of war and the conduct of large unit operations, those operations conducted by echelons above corps. This is in spite of the Army's long and successful history of such operations. There are many causes for this. Most have to do with the fact that the majority of this officer pool only experience tactical operations and that their military education only prepares them for tactical operations. The promotion process systemically culls out those individuals that do have such experience since assignment of a field grade officer to duty in an Army service component command is a death sentence when it comes to promotion to general officer.

The second reason is that joint and Army doctrine does not currently speak clearly and with one voice on this subject. Joint Publication (JP) 3-0, *Doctrine for Joint Operations*, does not totally agree with JP 3-10, *Doctrine for Joint Rear Area Operations,* on what constitutes operational force protection. Joint doctrine does not specifically state the doctrinal solution for which service will provide the Joint Rear Area Coordinator (JRAC) and his supporting command and control (C2) facilities. Since that doctrinal solution does not exist, no service provides the resources to conduct the responsibilities established in JP 3-10. Additionally, there is no Army equivalent publication to JP 3-10 since the rescinding of FM 90-14, *Rear Battle*, in 1989. (FM 3-90, *Tactics*, covers rear area and base security at the tactical level.) Future Army doctrine must be clear that the Army service component command (ASCC) will provide the Joint Rear Area Coordinator (JRAC). The Army's force management process will provide those resources once published doctrine establishes the requirement. This paper is an attempt to resolve this later problem and thus provide a firm conceptual foundation for those professional soldiers attempting self-development in the area of operational force protection beyond the limitations of their formal military education and experience.

Large Army units operate in a joint environment. Joint forces define force protection in the following manner. **Force protection consists of those actions to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information.**[1] The Army definition of force protection goes on to state: **These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporates the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against**

accidents, weather, or disease.[2] Army doctrine breaks down force protection into five major components. These five components are—

- Air, space, and missile defense.
- Nuclear, biological, and chemical defense.
- Antiterrorism.
- Defensive information operations.
- Security to operational forces and means.

Army commanders operating at the operational and theater-strategic levels participate in operations that span all five of these components of force protection established by FM 3-0 (100-5). The increased emphasis on force protection at every echelon stems from the conventional dominance of Army forces. Often unable to challenge the Army in conventional combat, adversaries seek to frustrate Army operations by resorting to asymmetric means, weapons, or tactics. Force protection counters these threats and minimizes losses to hostile action.

The Universal Joint Task List (UJTL) (CJCSM 3500.04B) serves as a common language and reference system for joint force commanders, combat support agencies, operational planners, combat developers, and trainers to communicate mission requirements. It is the basic language for development of a joint mission essential task list (JMETL) or agency mission essential task list (AMETL) that identifies required capabilities for mission success.[3] Table 1 illustrates the relationship between the Army's five components of force protection and the theater-strategic and operational force-protection tasks found in the UJTL. As shown in that table, the Army doctrine does not regard some UJTL force protection tasks as force protection tasks. The Army regards those tasks dealing with personnel recovery and the noncombatant evacuation as operations and they are the subject of separate manuals. (See Joint Publication (JP) 3-50.2, *Doctrine for Joint Combat Search and Rescue*, JP 3-50.3, *Joint Doctrine for Evasion and Recovery*, JP 3-07.5, *Joint TTP for Noncombatant Evacuation and Recovery*, and FM 3-07.5 (90-29), *Noncombatant Evacuation Operations*.) This chapter does not discuss these tasks since other manuals adequately discuss them. Minimizing safety and health risks within a theater of operations are specialized activities adequately discussed elsewhere in doctrine, and thus, not discussed in this chapter. (See JP 4-02, *Doctrine for Health Service Support in Joint Operations*, JP 4-04, *Joint Doctrine for Civil Engineering Support*, FM 3-34.211 (5-116), *Echelon Above Corps Engineer Operations*, FM 4-02 (8-10), *Health Service Support in a Theater of Operations*, and FM 4-02.17 (8-10-17), *Preventative Medicine Services*.) The remainder of this chapter will address the five components of force protection.

Army Components of Force Protection	Theater-Strategic Tasks		Operational Tasks	
Air, Space, and Missile Defense	ST 6.1	Provide Theater Missile Defense	OP 6.1	Provide Operational Air, Space, and Missile Defense
			OP 6.1.2	Integrate Joint/Multinational Operational Aerospace Defense
	ST 6.1.1	Process Theater Air and Space Targets	OP 6.1.1	Process and Allocate Operational Aerospace Targets
	ST 6.1.2	Provide Airspace Control Measures	OP 6.1.3.1	Employ Positive Control Measures
			OP 6.1.3.2	Employ Procedural Control Measures
	ST 6.1.3	Establish Theater Space System Force Enhancement Operations	OP 6.1.3	Provide Airspace Control
	ST 6.1.4	Organize and Coordinate Theater Air Defense	OP 6.1.4	Counter Enemy Air Attack (DCA) in the JOA
	ST 6.1.5	Organize and Coordinate Theater Missile Defense	OP 6.1.5	Conduct JOA Missile Defense
	ST 6.1.6	Support Tactical Warning and Attack Assessment in Theater	OP 6.1.6	Conduct Tactical Warning and Attack Assessment in the JOA
Antiterrorism	ST 8.4.2	Assist in Combating Terrorism	OP 6.2	Provide Protection for Operational Forces, Means, and Noncombatants
Security to Operational Forces and Means	ST 6.2	Coordinate Protection for Theater Forces and Means		
	ST 6.2.1	Coordinate the Preparation of Strategically Significant Defenses	OP 6.2.1	Prepare Operationally Significant Defenses
	ST 6.2.2	Coordinate the Removal of Strategically Significant Hazards	OP 6.2.2	Remove Operationally Significant Hazards
	ST 6.2.3	Protect Use of Electromagnetic Spectrum in the Theater	OP 6.2.3	Protect Use of Electromagnetic Spectrum in the JOA
	ST 6.2.4	Ensure Acoustic Protection	OP 6.2.4	Protect Use of the Acoustic Spectrum in the JOA
	ST 6.2.5	Establish and Coordinate Positive ID Procedures for Friendly Forces in Theater	OP 6.2.5	Provide Positive ID of Friendly Forces w/i JOA
	ST 6.2.6	Establish Security Procedures for Theater Forces and Means	OP 6.5	Provide Security for Operational Forces and Means
			OP 6.5.2	Protect and Secure Flanks, Rear Areas, and COMMX in the JOA
			OP 6.5.5	Integrate Host-Nation Security forces and Means
	ST 6.2.6.1	Establish and Coordinate Counterreconnaissance Theater-wide	OP 6.5.1	Provide Counterreconnaissance in the JOA
	ST 6.2.6.2	Establish and Coordinate Protection of Theater Install/Facilities, and Systems	OP 6.5.3	Protect/Secure Operationally Critical Installations, Facilities, and Systems
	ST 6.2.6.3	Establish and Coordinate Protection of Theater Air, Land, and Sea LOCs	OP 6.5.4	Protect and Secure Air, Land, and Sea LOCs in JOA
	ST 6.2.6.4	Establish and Coordinate Theater-wide Counterintelligence Requirements		
	ST 6.2.7	Initiate and Coordinate Personnel Recovery in Theater	OP 6.2.9	Coordinate and Conduct Personnel Recovery
	ST 6.2.7.1	Operate Theater Joint Search and Rescue Center (JSRC)		
	ST 6.2.7.2	Coordinate Civil Search and Rescue	OP 6.2.9.1	Provide Civil Search and Rescue
	ST 6.2.7.3	Coordinate Combat Search and Rescue		
	ST 6.2.7.4	Support Evasion and Escape in Theater	OP 6.2.9.3	Support Evasion and Escape in the JOA
Nuclear Biological, and Chemical Defense	ST 6.2.8	Establish NBC Defense in Theater	OP 6.2.8	Establish NBC Protection in the JOA
	ST 6.2.9	Minimize Safety and Health Risks	OP 6.2.10	Develop and Execute Actions to Control Pollution and Hazardous Materials
			OP 6.2.13	Conduct Countermine Activities
Defensive Information Operations			OP 6.2.11	Provide Counterdeception Operations
			OP 6.2.12	Provide Counter-Psychological Operations
	ST 6.3	Secure Theater Systems and Capabilities	OP 6.3	Protect Systems and Capabilities in the JOA
	ST 6.3.1	Employ Theater OPSEC	OP 6.2.14	Employ OPSEC in the JOA
			OP 6.3.1*	Employ OPSEC in the JOA
	ST 6.3.2	Employ Theater Electronic Security	OP 6.3.3	Employ Electronics Security in the JOA for Operational Forces
	ST 6.3.3	Supervise COMSEC	OP 6.3.2	Supervise COMSEC
	ST 6.3.4	Coordinate Concealment of Theater Forces/ Facilities	OP 6.3.5	Coordinate Concealment of Forces/Facilities
	ST 6.3.5	Protect Theater Information Systems	OP 6.3.4	Protect Information Systems in the JOA
	ST 6.4	Conduct Deception in Support of Theater Strategy and Campaigns	OP 6.4	Conduct Military Deception in Support of Subordinate Campaigns and Major Operations
	ST 6.4.1	Protect Details of Theater StrategyCampaign Plans/Operations	OP 6.4.1	Develop Operational Deception Plan
	ST 6.4.2	Misinform Adversary Regard. Conduct of Theater Strategy, Campaigns, and Unified Operations	OP 6.4.2	Conduct Operational Deception
	ST 6.4.3	Assess Effect of Theater Deception Plan	OP 6.4.3	Assess Effect of Operational Deception Plan
	ST 8.4.3	Conduct Evacuation & Repatriation of Noncombatants from Theater	OP 6.2.6	Conduct Evacuation of Noncombatant from JOA
			OP 6.2.7*	Establish Disaster Control Measures

*Tasks in Red Letters were found in the 1994 edition of CJCSM 3500.04B but have been moved in the 1999 edition

Table 1. Theater Strategic Force Protection Tasks Cross-walk with Operational Force Protection Tasks

AIR, SPACE, AND MISSILE DEFENSE

Air, space, and missile defense encompasses all activities focused on the identification, integration, and employment of forces supported by theater and national capabilities to detect, identify, locate, track, discriminate, minimize the effects of, and negate enemy air and missile threats. This includes the destruction of enemy aerospace systems prior to launch and in flight—along with their air, ground, or sea-based launch platforms and supporting infrastructure—during pre- and post-launch operations.

Air, space, and missile defense is inherently a joint mission. Its successful conduct requires a coordinated joint service effort. This coordination originates in the doctrine described in JP 3-01, *Joint Doctrine for Countering Air and Missile Threats* and supporting service publications. Air Force Doctrine Document 2-1.1 Counterair Operations describes the Air Force's contribution. Naval Warfare Publication 3-0.1 describes the Navy's contribution to joint TAMD. Marine Corps Warfighting Publication 3-25, *Control of Aircraft and Missiles* describes the Marine Corps' contribution. The Army's role is the focus of FM 3-01.12 (100-12), *Army Theater Missile Defense Operations*.

The purpose of air, space, and missile defense is to protect the joint force and allow its freedom of action. The continuing proliferation of advanced weapons and technology expands the scope and complexity of air, space, and missile defense efforts required to protect friendly forces within a theater of operations. The detection capabilities, engagement ranges, mobility, and lethality of air, space, and missile threats have significantly increased over what existed only a decade ago. Potential adversaries have access to advanced aircraft and missiles that can directly threaten US forces and international interests. They can now access space-based platforms that significantly augment their intelligence collection and communications capabilities. This growing diversity of aerospace threats requires joint forces to be more responsive, flexible, and integrated in their defensive efforts.

TAMD is composed of four operational elements: passive defense, active defense, attack operations, and C4I. Because of the continual proliferation of advanced air, space, and missile systems, any one technical solution cannot quickly counter all possible threats. The synergy achieved by coordinating and integrating all four operational elements into cohesive and coherent combat operations is the only way to counter them successfully.

ORGANIZATION OF FORCES FOR AIR, SPACE, AND MISSILE DEFENSE

The Joint Force Commander (JFC) normally designates the joint force air component commander (JFACC) as the supported commander for theater-wide counterair operations. Normally,

Normally, JFACC is the service component commander having the preponderance of air assets and the capability to plan, task, and control joint air operations. The JFACC will generally use centralized control and decentralized execution as the optimum arrangement to respond to air and missile threats. (See JP 3-01, JP 3-01.5, and JP 3-33 for more information on the JFACC role in theater-wide counterair operations.) (See Figure 1)

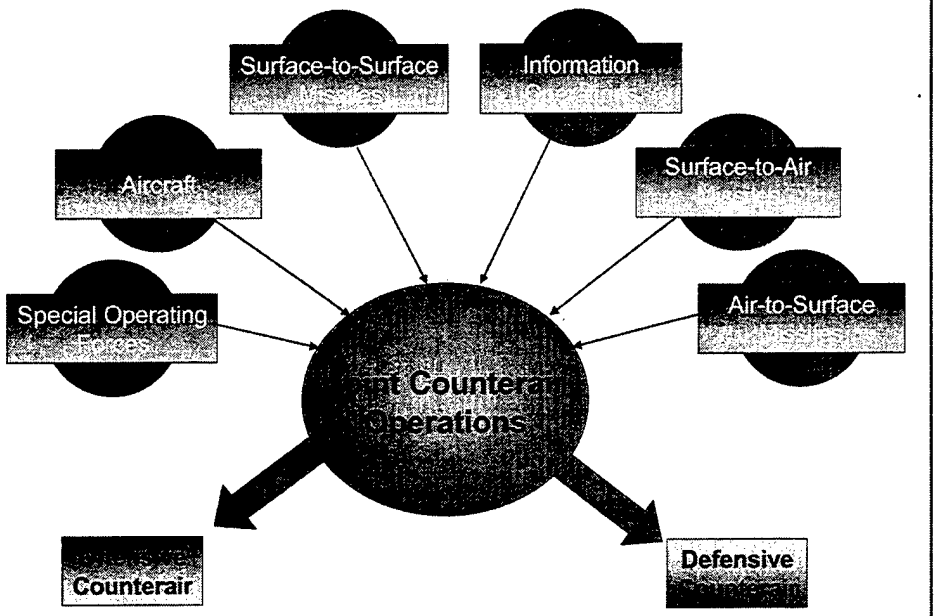


Figure 1. Joint Counterair Operations

The JFC will assign overall responsibility for air defense to a single area air defense commander (AADC). Normally, the AADC is the component commander with the preponderance of air defense capability and the command, control, communications, computers, and intelligence capability to plan, coordinate, and execute integrated air defense operations. This is normally the JFACC. Other Service components provide representation, as appropriate, to the AADC's headquarters. The JFC grants the AADC the necessary command authority to deconflict and control engagements and to exercise real-time battle management. Regardless of the command relationships established, all active defense forces made available for defensive counter air (DCA) are subject to the rules of engagement (ROE), airspace and weapons control measures, and fire control orders established by the AADC and approved by the JFC. The AADC's primary responsibilities include:

- Integrating AD forces and operations to defend the joint force against enemy air and missile attack.
- Developing, integrating, and distributing a JFC-approved joint air defense plan (ADP).
- Developing and executing—in coordination with the JFC staff's operations directorate (J3) and command, control, communications, and computers (C4)

directorate (J6)—a detailed plan to disseminate timely air and missile warning and cueing information to component forces, allies, coalition partners, and civil authorities, as appropriate.

- Developing and implementing identification and engagement procedures appropriate to the air and missile threat.
- Ensuring timely and accurate track reporting among participating units to provide a consistently common operational picture.
- Establishing sectors or regions, as appropriate, to enhance decentralized execution of DCA operations.[4]

The Army Air and Missile Defense Command (AAMDC) is the Army organization that performs critical theater level air and missile defense planning integration, coordination, and execution functions for the ARFOR Commander and JFLCC. The AAMDC integrates the four operational elements of TMD: active defense, attack operations, passive defense, and C4I to protect contingency, forward deployed, and reinforcing forces as well as designated theater strategic assets. The AAMDC prepares the air and missile defense annex for the ARFOR operations order (OPORD). The AAMDC commands the echelon above corps (EAC) ADA brigades and other assigned forces.

The AAMDC provides the staff and equipment to plan, coordinate, deconflict, and monitor the execution of the ARFOR Commander's (or JFLCC's if designated) air, space, and missile defense TMD plans during force projection operations. The AAMDC consists of intelligence, fire support, aviation, chemical, ADA, Special Forces, and signal personnel melded into one organization. The AAMDC focuses on air, space, and missile defense operations for the ARFOR Commander (or JFLCC if designated) and is continuously collecting intelligence, analyzing information, and coordinating missions across all air, space, and missile defense operational elements. For example, the AAMDC coordinates with the ARFOR G2, G3, and Deep Operations Coordination Cell (DOCC) to recommend prioritized TMD targets. In addition, AAMDC LNOs deploy to all major theater elements: JFC, JFACC/AADC, JFLCC, Joint Force Maritime Component Commander (JFMCC), Joint Special Operations Task Force (JSOTF), Battlefield Coordination Detachment (BCD), DOCC, ACE, and multinational headquarters to coordinate and deconflict the execution of integrated air, space, and missile defense operations.

When an AAMDC deploys to a theater of operations, its commander performs the functions of Theater Army Air and Missile Defense Coordinator (TAAMDCOORD) and Deputy Area Air Defense Commander (DAADC) as required. The TAAMDCOORD is the Army Air and Mis-

sile Defense Coordinator (AMDCOORD) to the ARFOR Commander (or JFLCC if designated), JFACC, and the AADC.

The TAAMDCOORD, as a special staff officer to the ARFOR Commander (or JFLCC if designated), ensures Army air and missile defense is integrated with active air defense operations and planning at the theater level. His specific functions are—

- Plans theater air and missile defense force projection and sustainment operations.
- Integrates the air defense communications systems with the AADC and operational-level ADA brigades, corps, air operations center (AOC), BCD, control and reporting center (CRC), and AWACS (airborne warning and control system).
- Coordinates the theater air and missile defense linkages with the JFACC, joint force maritime component commander (JFMCC), and multinational ADA forces. These linkages include interface with intelligence sources, offensive counter air, space operations, and logistics.
- Trains and evaluates all Army ADA organizations assigned to operational-level air defense units.
- Recommends priorities for allocation of logistics requirements (manning, arming, fixing/maintaining, moving, fueling, and soldier sustainment) for all ADA organizations within the theater.
- Identifies and recommends pre-positioning of war reserve materiel stocks related to air defense missions.[5]

The functions of the DAADC are:

- Integrate Army TMD active defense and ADA forces with joint active air defense operations.
- Advise the AADC regarding weapons control procedures and measures, air defense warnings (ADW), and emission control (EMCON) measures.
- Assist the AADC in the air defense plan development.
- Advise the AADC on matters regarding active missile defense operations and ensure integration into active air defense plan.
- Advise the AADC on TMD operations and integrate active defense planning.
- Advise the AADC on ADA weapons capabilities and limitations.[6]

Units at the operational-level capable of conducting active defense normally consist of at least one EAC ADA brigade that provides C2 for one or more PATRIOT battalions or air and missile defense task forces (AMDTF) and battalions. These task forces may consist of Avenger,

PATRIOT, and Theater High Altitude Area Defense (THAAD) fire units. ADA units at this level receive missions from the AAMDC to defend the force and critical assets prioritized on the CINC's DAL (at the joint level there are DALs; however, at the Army and lower levels there are air and missile defense priorities).

Corps active defense units normally consist of an ADA brigade that provides C2 over assigned ADA battalions. The corps ADA brigade commander task organizes his resources to protect the corps and division commander's air and missile defense priorities. Corps/division ADA units receive missions from the corps commander to protect forces and critical assets. See FM 3-01.12 (100-12), *Army Theater Missile Defense Operations.*

CONTROL MEASURES FOR AIR, SPACE, AND MISSILE DEFENSE

Airspace control increases the operational effectiveness of air, space, and missile defense by promoting the safe, efficient, and flexible use of airspace. Airspace control permits greater flexibility of operations. Establishing direct controls minimize mutual interference between air, space, and missile defense operations and other joint force operations. Airspace control consists of the coordination, integration, and regulation of the use of airspace with defined dimensions. Within the theater of operations of a joint force, the JFC assigns overall responsibility and authority for airspace control to one component commander. The mission of the airspace control authority is to coordinate and integrate the use of airspace within the joint AO. Because of the close relationship between airspace control and air, space, and missile defense, the airspace control authority (ACA) is normally the AADC. Subject to the authority of the joint force commander, the ACA establishes the broad policies and procedures for airspace control operations and coordination among units operating in the airspace control area.

Airspace control measures afford the ACA the means to procedurally or positively control all airspace users. Airspace control measures are rules to reserve airspace for specific users, restrict actions of airspace users, control actions of specific airspace users, or require airspace users to accomplish specific actions. The ACA implements the airspace control measures through the theater airspace control plan and specific directives. The AMDCOORD and A2C2 element at each echelon provide Army requirements to the BCD at the joint air operations center for incorporation into the airspace control plan.

Identification is an important function of airspace control in air, space, and missile defense operations. Hostile and friendly identification ensures timely engagement of targets and reduces the potential for fratricide. The tactical situation, electronic interference, or equipment malfunction may preclude positive friendly identification, but airspace control measures provide a

procedural backup. From an ADA perspective, many airspace control measures provide a means of probable friendly identification and default hostile identification. These measures allow friendly forces optimum use of airspace while minimizing the risk of engagement by friendly air defense. Examples are minimum risk routes and standard-use Army aircraft flight routes and air corridors.

Airspace control measures afford commanders the means to control airspace use, protect ground operations or facilities, and control other users of the airspace. High-density airspace control zones and restricted operations zones are examples of supplemental fire control measures. Other important control measures include the locations of the fire support coordination line (FSCL), coordinated fire lines (CFLs), engagement boxes, restricted fire areas (RFAs), and no-fire areas (NFAs). The targeting plan and the assignment of targeting numbers plays a role in airspace control measures as are high priority targets, target selection standards—range, target location errors (TLEs), and attack guidance for preemptive strikes.[7] See Joint Pub 3-52 and FM 3-52 (which consolidates information previously found in FMs 100-103 and 100-103-1) for further information on airspace control measures.[8]

PLANNING FOR AIR, SPACE, AND MISSILE DEFENSE

Planning air, space, and missile defense operations involves analyzing the mission, performing a defense lay down, assigning missions to subordinate brigades, and performing follow up coordination to ensure that forces and selected geopolitical assets remain adequately protected. Planners first review the assigned mission and identify the critical assets to be protected. The JFC identifies these assets in his approved defended asset list (DAL). The DAL is a prioritized listing of assets by phase and is included in the OPLAN and air defense plan. The enemy situation is appraised by reviewing the IPB and recent intelligence information to confirm enemy COAs and determine the types and numbers of missiles and aircraft the enemy is likely to employ, the locations of launch sites, and the ranges of these sites from the assets to be defended. Planners must also review the composition and disposition of the AMD resources available to protect critical assets.

After analyzing the mission, the AAMDC operations staff performs a defense lay down to determine if available air and missile defense resources can adequately protect critical assets. The operations staff does this by the use of available automated planning tools. They use them to plot the locations of enemy launch sites, protected assets, and air and missile defense unit locations to determine degree of achievement of the required surveillance and engagement coverages and levels of protection. If required coverages or levels of protection cannot be

achieved with available air and missile defense resources, additional resources must be requested from the ARFOR commander or the JFC, and other component commanders must be advised of the risk to their forces or assets.

Planners task-organize the EAC ADA brigades and then assign specific assets to the brigades for protection. The brigades then perform more detailed planning to determine which subordinate battalions and task forces will cover the assets. Throughout operations, active air defense planners coordinate with the ADA brigades to ensure the availability of sufficient air and missile defense resources to accomplish the mission and weighted coverages in accordance with the JFC's priorities.

As required by METT-TC, the AAMDC may establish or participate in re-prioritization boards to recommend changes to air and missile defense priorities on the DAL and adjustments to the defense design during the course of operations. The board uses an objective process that quantifies the level of importance of each asset based on selected criteria. Criteria are weighted based on consideration of the JFC's guidance and intent and his center-of-gravity concerns. Board recommendations are forwarded to the respective component commanders and the AADC, and are ultimately approved by the JFC. The AADC may designate the AAMDC commander (in his capacity as the DAADC) to chair the joint re-prioritization board.[9]

The AAMDC has a strong supporting role in TAMD IPB attack strategy development, and the target development process. The attack operations cell in coordination with AAMDC intelligence personnel and the analysis and control element (ACE) provide detailed target intelligence to the DOCC and recommend offense counter air attack strategy and plans. AAMDC intelligence personnel assist the ACE in the air, space, and missile portion of the IPB effort by providing dedicated analysts and subject matter experts.

The AAMDC G2 may deploy to the ACE a liaison team equipped with the necessary equipment to establish connectivity to intelligence resources. If deployed, the LNO team collects information for the AAMDC and passes information requirements to the ACE collection manager. Recommendations for collection support for TAMD IPB are made to the ACE for incorporation in the joint force collection strategy. The G2 analysis section supports the attack operations cell by analyzing launch events, conducting counter-mobility analyses, refining and validating the IPB, nominating deliberate targets 72-96 hours out, analyzing post-launch events, building tracking profiles, and disseminating intelligence products and reports for the ARFOR commander or JFLCC.

The AAMDC G2 leverages all intelligence sources to develop a comprehensive air, space, and missile intelligence picture. AAMDC G2 personnel may establish intelligence collaboration

efforts with their intelligence counterparts at the JAOC through digital and voice means or the AAMDC LNO team deployed to support the DAADC and AADC. TM analysts in the AAMDC G2 section and the JAOC may collaborate in AMD IPB development and share near-real time target intelligence. Intelligence collaboration between component TMD nodes ensures that all available TM information is fused, limited collection resources are efficiently used, and operational level decision-makers have the best analysis available.

At the Joint Task Force (JTF) level, the JFC issues targeting guidance and priorities to establish how air- and surface-delivered fires will accomplish his objectives. When established, the joint targeting coordination board (JTCB) assists the JFC in providing targeting guidance and priorities for the campaign. The AAMDC commander should be a member of the JTCB to provide a TM focus to the process. The JFACC Staff at the JAOC is heavily involved in the JFC's campaign through the production and execution of the Air Tasking Order (ATO). The ATO ultimately assigns aircraft and weapons against targets and runs for a theater-specific period, usually 24 hours. The length of the ATO development cycle is also theater-specific, but usually ranges between 48- and 96-hours. The ARFOR DOCC is responsible for coordinating ARFOR deep operations and targeting outside the ARFOR AO with the ATO planners at the JAOC. Targets identified for attack by the AAMDC G2 and attack operations section are nominated to the DOCC for prosecution, either as preplanned targets or immediate targets.[10]

PREPARING FOR AIR, SPACE, AND MISSILE DEFENSE

Commanders at all levels ensure their units take the appropriate passive defense measures to execute force protection as part of the preparation process. The establishment of an integrated C4I system is necessary to integrate all the elements of JTMD at the Army, joint, and multinational level. Army air and missile defense elements form a cohesive JTMD force with the other components and multinational forces that is synchronized, integrated, synergistic, fused, and seamless to provide protection of theater forces and critical assets.

Defensive counter-air preparations begin prior to deployment with the IPB and the development of an area air defense plan. Continuous surveillance is required for early detection, identification, and prediction of attack areas of air and missile threats. The integration of active air defense systems provides efficient control and exchange of essential near real time information to all defensive forces and resources. The development of plans and communications architecture to warn forces and cue appropriate sensor and air defense systems to threats is critical.

Many ADA units have unique and powerful signatures. Deception operations frequently employ them in support, since ADA units are vital to force protection. Equally important, whenever possible ADA units should take actions that deceive threat RSTA as to their own locations and capabilities.

A rehearsal is the process of practicing a plan before actual execution. Rehearsing key combat actions allows participants to become familiar with the operation and to visualize the plan. Rehearsals assist units in orienting themselves to their environment and to other units during execution. Rehearsals provide an opportunity for subordinate leaders to analyze and understand the plan. Rehearsals also provide a forum to "proof" the plan, which validates its feasibility, logic, and adequacy of battle command measures. Rehearsals with combat units usually occur at the tactical level, while operational level headquarters can rehearse key aspects of a plan using command post exercises. Even if time does not permit a complete rehearsal with a full complement of troops and equipment, some form of rehearsal must take place with all key leaders. ADA commanders and leaders must conduct some form of rehearsal with their units. They must also participate in the rehearsal of the supported units. They use time management techniques to accomplish both tasks.[11]

EXECUTION OF AIR, SPACE, AND MISSILE DEFENSE

To execute this mission, joint force commanders (JFCs) integrate the capabilities of each of their Service components to conduct offensive and defensive operations. (See Figure 2.) Army, national, and theater intelligence, surveillance, and reconnaissance (ISR) assets detect and track the movement of aerial threats, theater missile launch platforms,

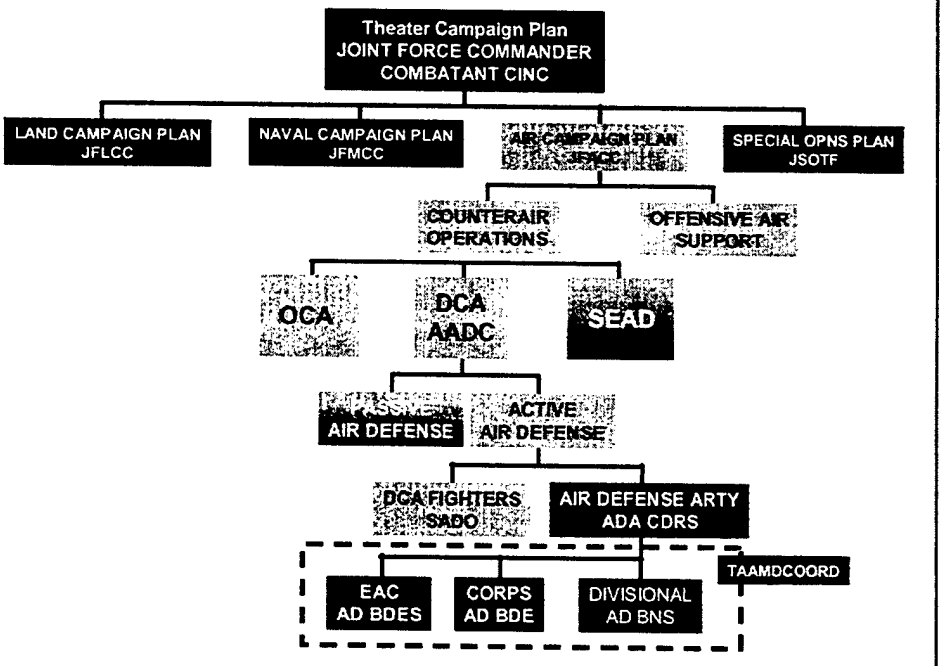


FIGURE 2. THEATER ORGANIZATION FOR AIR, SPACE, AND MISSILE DEFENSE

cue active joint air and missile defense and attack operation forces for engagements, and warn the force of missile launches. Offensive counterair (OCA) operations seek to dominate the enemy's air power and prevent the launch of threats. Army aviation and fire support units provide the JFACC (supported commander for OCA attack operations) with responsive attack operations capabilities to complement friendly offensive aircraft and cruise missiles (CMs). Conventional Army forces do not normally participate in OCA operations. Army special operating forces conducting one or more of their seven primary missions—unconventional warfare, foreign internal defense, information operations, counterproliferation, direct action, special reconnaissance, and combating terrorism—may conduct activities that impact on the conduct of OCA by the joint force. Of course, conventional forces capture or destroy enemy aircraft and missiles encountered on the ground and associated supporting infrastructure when allowed by the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). How the joint force commander (JFC) organizes his forces directly influences the ability of those joint forces to meet the threat. Unity of effort, centralized planning, and decentralized execution are key considerations.

The JFC may provide service component capabilities to the JFACC or AADC for counterair missions. The JFC determines the most appropriate command authority over forces made available in this case. Normally for DCA, air sorties are provided TACON, while surface-based active defense forces are provided in direct support.

Army forces within a theater of operations have a large role in the conduct of defensive counterair (DCA) operations. DCA is all defensive measures designed to detect, identify, intercept, and destroy or negate enemy forces attempting to attack or penetrate the friendly air envi-

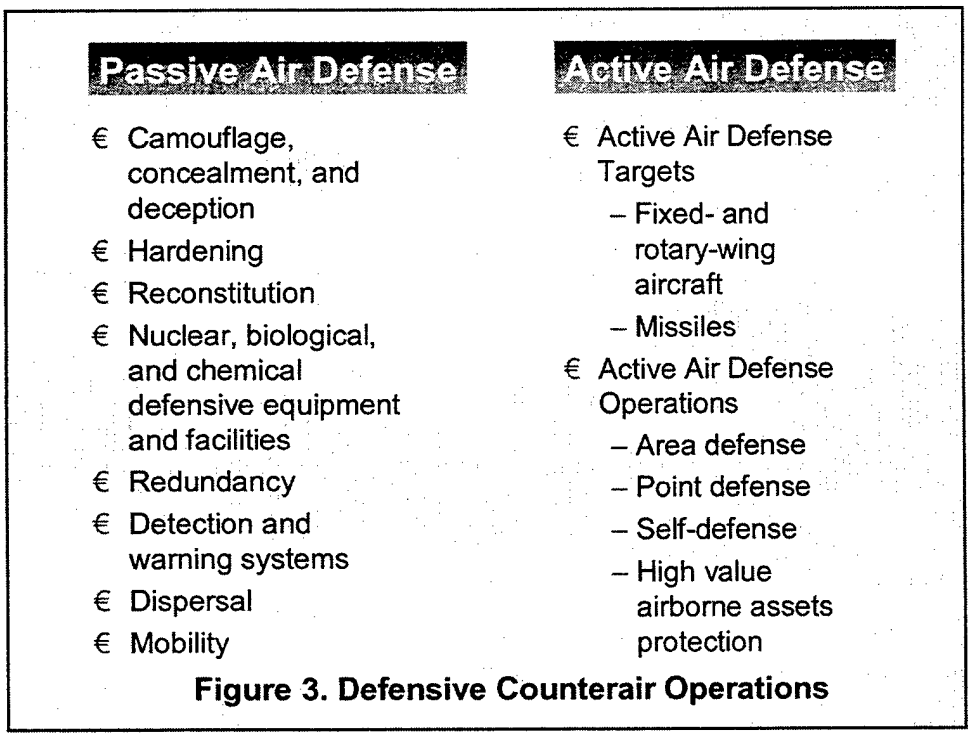


Figure 3. Defensive Counterair Operations

ronment.[12] These operations include both active and passive air defense measures. (See Figure 3.) DCA operations employ a mix of weapon and sensor systems from all components. Army air and missile defense systems execute a major role in active defense and a supporting role in attack operations. The goal of DCA operations, in concert with offensive operations, is to provide a secure area from which joint forces can operate. The JFC establishes and the AADC implements air and missile defense priorities through promulgation of an area air defense plan. The defense criteria is normally to detect, identify, intercept, and destroy the threat. Since DCA operations employ weapons and sensor systems within the same airspace, these operations are subject to the AADC's weapons control procedures and measures and integrated with the JFACC's overall plan for the conduct of air operations.

Active Air Defense is direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets. These actions protect friendly forces and facilities by negating the threat while in flight. Active air defense measures include layered defense-in-depth against air and missile threats through multiple engagement opportunities. Integrated detection, identification, assessment, interception, and engagement system for air and missile threats is necessary to protect friendly forces and vital interests. This integrated active air defense system includes the use of aircraft, air defense weapons, electronic warfare (EW), and other available weapons. Integration of these weapon systems allows for multiple engagements of an aerial threat, thus providing a defense in depth.

Active air defense measures include area defense, which uses a combination of weapon systems to defend broad areas; point defense to protect limited areas (normally vital elements or installations); and self-defense, where friendly forces use organic weapons and systems. Active measures may also include high value airborne asset (HVAA) protection. HVAA protection uses fighter aircraft to protect critical airborne platforms, such as the Airborne Warning and Control System.

Passive air defense provides individual and collective protection of friendly forces and critical assets. Passive air defense is the responsibility of commanders at all levels of the joint force. The AADC should provide timely attack warning, which initiates many of the passive defense measures. General warnings indicate that attacks are imminent or have occurred. Specific warnings signify that specific units or areas are in danger of attack. Passive defense measures include camouflage, concealment, deception, hardening, reconstruction, nuclear, biological, and chemical defensive equipment and facilities, redundancy, detection and warning systems, mobility, and dispersal.

While preplanned targets are an integral part of an overall air, space, and missile attack strategy, immediate targeting is also essential to the successful conduct of air, space, and missile attack operations. Air, space, and missile IPB does not stop after planning. It is a systematic, continuous process of analyzing the threat and environment. This analysis refines target areas and focuses collections so that ultimately, short dwell or immediate targets become identifiable and engageable. Immediate targets—those that must be attacked inside the normal ATO planning cycle—are also submitted to the DOCC via a request and nominations process similar to that used for preplanned targets. Examples of immediate targets are mobile forward operating bases (FOBs), missile transload sites, transporter-erector launcher (TEL) hide sites, and launch sites. When identified by the AAMDC, these targets are forwarded to the DOCC fire support element (FSE), which processes the request. If the request is approved and the target is serviceable with Army assets, it is forwarded to the BCD for airspace clearance and to the executing unit for attack. If not serviceable by Army assets, the BCD receives the request and passes it to the execution cell in the combat operations division of the JAOC for tasking to available aircraft. The AAMDC may have attack operations LNOs deployed at the DOCC and the BCD/JAOC to facilitate TMD attack operations and keep the attack operations cell informed of the status of target nominations and all available attack assets.[13]

The passive defense cell tracks friendly forces and monitors ARFOR or JFLCC ground and TAMD operations to assist it in performing its primary function of disseminating warnings to the force. The cell also monitors the DAL and active air defense operations conducted to protect priority assets. Reports of enemy air activity and missile launches are provided digitally by several joint sources in near real time to information workstations within the cell. The workstations display the air and missile activity including the number of enemy air sorties, missiles launched, launch locations, and predicted impact areas and times.

Other workstations receive reports of NBC events and display the type of event, type of burst or agent, area of contamination, downwind hazard, and the units affected. The cell has the ability to predict ground effects of WMD from identified incoming theater ballistic missiles and pass that information immediately to affected units. An integrated warning system throughout the entire theater of operation disseminates tactical warning and attack assessments to threatened units. Passive defense cell personnel also can receive joint force information, intelligence information, and weather data to aid in current operational decisions. The passive defense cell disseminates general and specific warnings based on receipt of the above information.[14]

The employment of defensive weapon systems requires early identification of friendly, neutral, or hostile aircraft and missiles to maximize beyond-visual-range engagement and avoid

fratricide. This requires clearly understood rules of engagement (ROE). The problem of distinguishing friendly, neutral, and enemy assets while employing various weapon systems against the latter is a highly complex task for some threats. However since ballistic missiles have a distinct flight profile, ROE for this threat should allow immediate engagement. The AADC and ACA establish procedures within the airspace control system to identify positively all airborne assets, reduce delays in operations, and prevent fratricide. Positive identification (ID) of tracks is normally the preferred method of operation. In the absence of positive ID, procedural ID is used, which employs previously established and promulgated airspace control measures. Generally, units use some combination of positive and procedural ID.

Early warning of hostile air and missile attacks is vital for a layered defense. DCA operations attempt interception of intruding enemy aircraft and missiles as early as possible. Although DCA operations are reactive in nature, they should be conducted as far from the friendly operational area as feasible. To maximize destruction of enemy air and missile threats, the engagement process must continue throughout the threat's approach to, entry into, and departure from the friendly operational area. The AAMDC fire direction center identifies air, space, and missile threats to the joint force, processes flight-tracking information, and allocates targets for friendly systems. This ensures freedom of action for campaigns and major operations and the protection of key assets.

Surface-to-air weapons offer high firepower and rapid responsiveness. Their effectiveness requires a reliable, interoperable interface with aircraft operations. Integration of these capabilities strengthens mutual support and provides the best overall defensive coverage.

NUCLEAR, BIOLOGICAL, AND CHEMICAL DEFENSE

Campaign and supporting plans must include options for the continued generation of adequate and timely force capabilities in the event of enemy use of NBC weapons within the supported combatant commands area of responsibility. Army commanders operating at the theater-strategic and operational levels must establish priority intelligence requirements, take pre-crisis actions to deter or prevent an enemy's employment of NBC weapons, plan counterforce and active defense operations to prevent or minimize NBC attacks, and plan actions to counter, mitigate, and manage the effects of an NBC attack. In conjunction with host countries, particular emphasis should be placed on early warning and detection; actions to prepare US and indigenous military forces; and protection of threatened civilian populations, essential infrastructures, and facilities. ARFOR commanders should also develop and exercise plans to

support host country actions to minimize and manage the effects of an NBC attack, especially where the effects may constrain US military freedom of action.[15]

All Army elements and commands within a theater of operations have basic goals at the outset of operations. (See Figure 4). A key task is the establishment of protection against NBC attacks in the operational area and in other areas providing forces and sustaining capabilities. The goals established to carry out military responsibilities in this phase of operations include prevention of adversarial use of NBC weapons in the United States or abroad, rapid and uninterrupted force preparation and deployment, and comprehensive force protection. Joint operations planning, development of branches in campaign plans, redundant assignments of mission essential tasks to forces, and visible exercises that ensure peacetime preparedness reflect these goals and may thereby deter potential opponents.[16] The joint principles of operations in NBC environment—deterrence, assuring sustained combat operations, and public diplomacy and information apply at the ARFOR level.[17] The joint and Army principles of NBC defense—avoidance, protection, and decontamination—also apply at the ARFOR level.[18]

ORGANIZATION OF FORCES

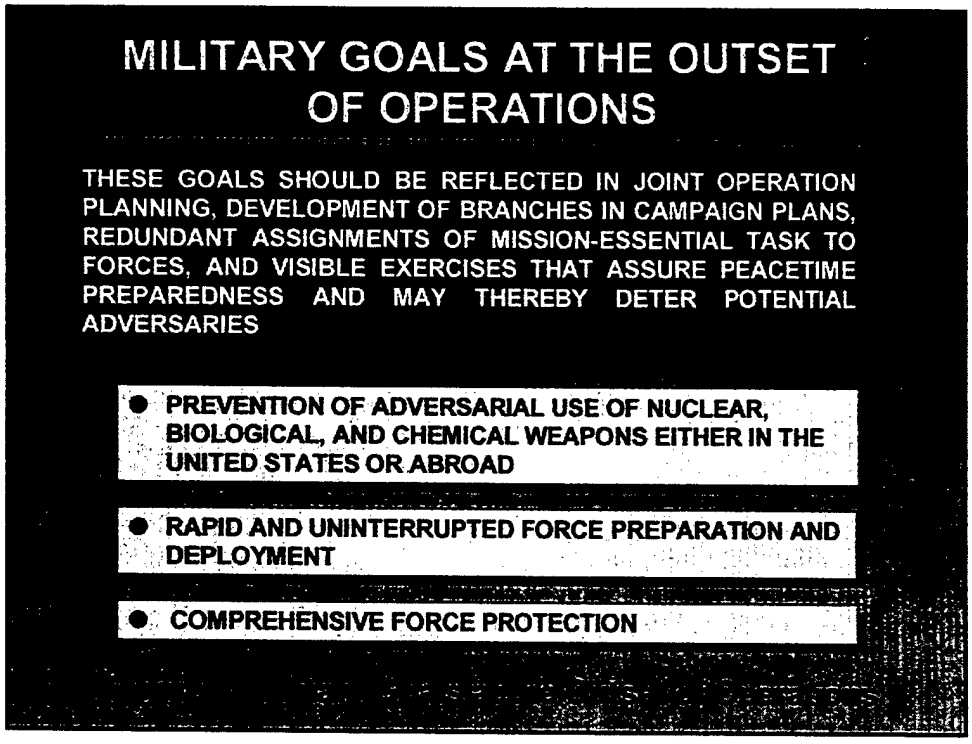
Army chemical units are indispensable to theater NBC operations. They offer a range of capabilities necessary to a versatile force. They can support operations as individuals, teams, or units. A mix of different units (decontamination units, NBC reconnaissance elements, smoke units, and biological defense units) is often necessary to achieve the proper balance of capabilities-force protection and mission accomplishment. Forces deployed in countries with WMD or chemical industrial complexes require support from both NBC battle staffs and units. They provide training support and technological and consultative operations for nuclear accident- and incident-response operations and chemical accident- and incident-response operations that involve NBC material, flammable and combustible substances, and industrial chemical hazards. In addition, the U.S. Army Nuclear and Chemical Agency (USANCA) provides nuclear employment augmentation teams (NEAT) to support land component commanders in tactical nuclear weapons targeting and consequence analysis.[19]

In a major theater of war (MTW) or Smaller Scale Contingency (SSC), NBC defense and smoke/obscurant units are task-organized into battalions either on an area or functional basis based on METT-TC. Chemical companies are not permanently assigned to battalion headquarters in order to maintain a high level of flexibility in the contingency operations. Area-based battalions would have mixture NBC defense and smoke units assigned. Functionally based battalions conduct either NBC defense or smoke/obscurant missions.

The NBC force organization within a theater depends greatly on the threat. US forces are organized and trained to operate against a sophisticated threat capable of employing NBC munitions. Based upon the actual factors of METT-TC prevailing in the theater, the ASCC commander tailors his available NBC forces to meet the specific situation. He normally assigns NBC defense responsibilities in a contingency to a subordinate unit: an ARFOR, a corps, or theater support command. Frequently, an active duty chemical battalion will provide NBC support for a larger force until reserve component units can arrive. Early arriving NBC units must be aware of the large area occupied by tactical units as well as the Army rear area or joint rear area (JRA). The senior chemical unit commander, his staff, and the functional units assigned normally perform NBC missions in support of the joint force in addition to their own service.[20]

The ASCC/ARFOR normally allocates theater NBC defense and smoke/obscurant units in mature theater in the following manner:

- One NBC Reconnaissance Company per theater
- One Bio-Detection Company per theater
- One Dual-purpose NBC Reconnaissance/Decontamination Company per SPOD
- Four Dual-purpose Smoke/Decontamination Companies per theater
- One Dual-purpose Smoke/Decontamination Company per USAF airfield
- One Dual-purpose Smoke/Decontamination Company per APOD
- One Dual-purpose Smoke/Decontamination Company per SPOD



Approximately 15 percent of all chemical units are in the active component. The majority are assigned to the U.S. Army Reserve and are located in every region of the United States. As a result, the number of NBC defense and smoke units available to support the COMMZ and JRA may be inadequate, at least initially, until the NCA orders unit activations.

As the theater matures, the ARFOR commander organizes incoming chemical units into chemical battalions and chemical brigades. A typical allocation of theater chemical brigades is as follows—

- One chemical brigade is retained by the ASCC/ARFOR and is OPCON to the Deputy Commanding General for Support (DCG(S)/Deputy Joint Rear Area Coordinator (DJRAC) or is assigned to the Theater Support Command (TSC)
- One chemical brigade is assigned to each army corps
- One chemical brigade is attached to a MEF (when directed).

Figure 5 shows the command and control relationship between the ASCC/ARFOR, the chemical brigades, and supported units.[21] FM 3-11 (3-100) documents the exact capabilities of chemical organizations and the assigned responsibilities of chemical staff officers at different echelons.[22]

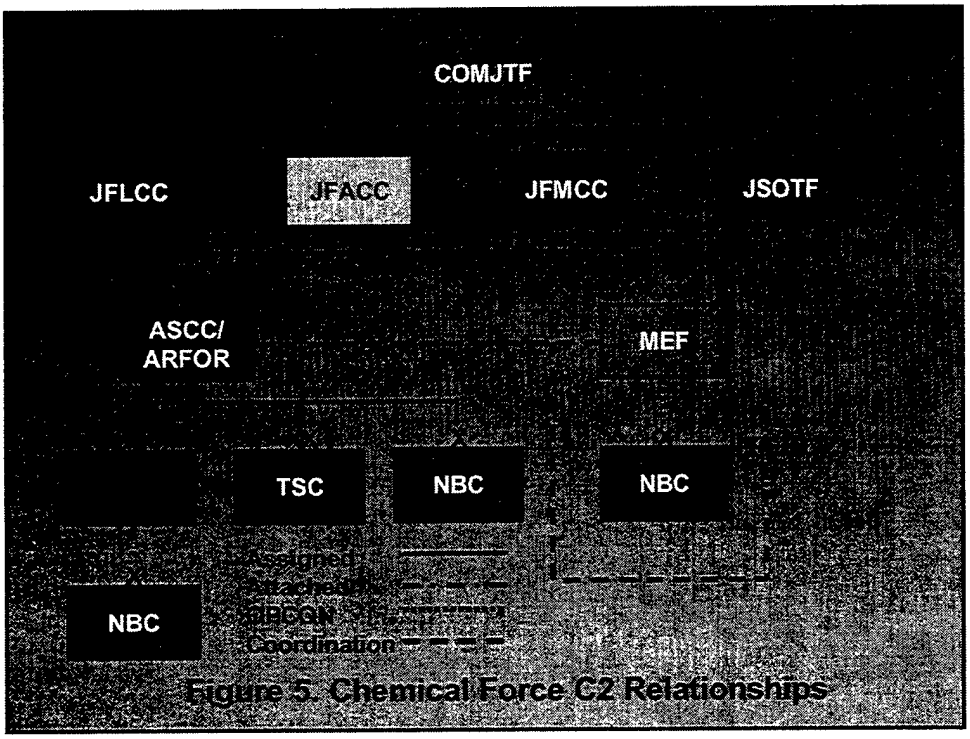


Figure 5. Chemical Force C2 Relationships

CONTROL MEASURES

The control measures associated with NBC defense at the theater-strategic and operational are the same measures used in other theater operations. They include the designation of command and support relationships and areas of operations for various units, such as the joint rear area, bases, and base clusters. The Joint Rear Area Coordinator (JRAC) normally designates air- and sea-ports of embarkation and debarkation as bases. The standardized reporting requirement of the Nuclear, Biological, and Chemical Warning and Reporting System (NBCWRS) is a type of control measure as are the various stages of Mission Oriented Protective Posture (MOPP). FM 3-0 (100-5) defines the area of operations. FM 3-90 defines bases

and base clusters, FM 3-11 (3-100) defines and discusses the NBCWRS and MOPP in great detail.

PLANNING CONSIDERATIONS FOR NBC DEFENSE

The JFC must plan for and integrate US and multinational force capabilities to sustain the multinational operational tempo in all mediums (air, sea, land, and space), regardless of the nature and targets of an adversary's NBC attack. The JFC will establish and implement a deliberate process for assessing the vulnerability of manpower and materiel to NBC attack. This process will integrate all offensive and defensive capabilities to reduce the threat of NBC use and sustain operations if attacks occur. The process will also include executing mitigation and restoration plans to reduce the operational impact of NBC contamination and other toxic hazards.[23]

Theater-level logistic support is generally furnished from Service-operated and other functional fixed sites throughout the JRA. Logistic NBC defense operations in the JRA are based on Service and site requirements, but will be coordinated with the joint rear area coordinator (JRAC) and base cluster commanders (when designated). One of the JRAC's responsibilities is NBC defense integration. Component commanders will incorporate NBC plans, exercises, equipment considerations, individual decontamination measures, and preventive measures into their area and base cluster defense plans. They will also position NBC defense personnel and assets to support current mission requirements and facilitate future operations, in accordance with JFC and area commander directives and priorities.[24]

Combatant commanders must be able to execute the campaign under NBC conditions through unified action at the theater level. Unified action for subordinate JFCs is equally important for combat, combat support, and combat service support units of all Services and multinational partners. Unified action encompasses not only NBC-related actions but also all other actions that permit continuation of theater operations and focus on attaining the single theater military objective in line with the JFC's intent.[25]

NBC defense force structure and force development activities are the responsibility of individual Services and USSOCOM. Combatant commanders remain aware of the salient factors that pertain to NBC defense requirements and USSOCOM or Service components' responses to their requirements through the Joint Operation Planning and Execution System. The combatant commander is responsible for ensuring proper placement of NBC defense assets in theater in advance of a crisis or conflict, and in the time-phased force and deployment data prepared to support movement to the theater. In particular, the combatant commander should be cognizant

of any significant shortfalls in the capability or availability of NBC defense assets. See JP 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments.*[26]

PREPARATION CONSIDERATIONS FOR NBC DEFENSE

Responsibility for preparations that allows the execution of these NBC defense plans relies heavily on the JRAC and base cluster commanders. These responsibilities may change based on specific command and/or mission requirements. The JRAC, as defined in JP 3-10, is responsible for coordinating the overall security and area damage control efforts of the JRA. (See Figure 6.) Specifically, the JRAC incorporates provisions and procedures for NBC defense to include warning and reporting procedures. His general JRA coordination responsibilities include—

Figure 6. JRAC Specific Responsibilities

- Coordinates JRA security.
- Positions NBC protection assets
- Integrates security
- Conserves resources
- Prevents support degradation
- Establishes joint rear tactical operations center (if required) with joint intelligence center interface.[27]

The JRAC ensures that joint rear area commanders and staffs incorporate appropriate NBC planning, exercises, equipment, personnel decontamination measures, and preventive measures into overall security planning and operations throughout the joint rear area. Component commanders should also ensure appropriate memorandum of understanding (MOU) and interservice support agreements (ISSA) address NBC and force protection matters including specific military unit responsibilities under varying conditions. In addition, appropriate MOU and

ISSA should be in place prior to actual operations. Component commanders are also required to incorporate NBC defense planning, exercises, equipment, personnel decontamination measures, and preventive measures into the overall security planning and operations throughout the joint rear area.[28]

Fixed sites will fall into a base or base cluster category depending on geographical dispersion, activities, and functions. For example, a port designated as a base cluster might consist of berthing, railhead, and marshaling area bases; all part of a synchronized port NBC defense plan. In turn, the base cluster commander controls and coordinates the base defense plans of separate base commanders. Each base commander develops plans that include an NBC defense annex and may also include a CCD or smoke annex. FM 3-90, JP 3-10 and JP 3-10.1 address additional details on base defense.[29]

The speed at which NBC reconnaissance occurs directly influences fixed site operations. Toward that end, the entire base populace should be involved. Individuals are responsible for surveying their immediate work area. Shelter management teams (SMTs) are responsible for checking pre-positioned NBC detection assets (M8/M9 paper, automatic liquid agent detectors, etc.) in and around their facility. Specialized teams or personnel complete preassigned reconnaissance.[30]

Transient commanders located near fixed sites may be required to support base defense with their organic assets, including NBC defense capabilities. In force projection operations, commanders quickly move combat power away from the POD to reduce force vulnerability. However, since combat sustainment flows through the POD, the transient commander has a vested interest in assisting with NBC defense emergencies.[31]

Tenant commanders of forces assigned to a base cluster/base retain responsibility for unit protection and NBC defense. However, tenant commanders may also be tasked to—

- Help prepare/integrate base defense plans.
- Conduct and/or support individual, unit, or US/HN civilian NBC defense training.
- Provide BDOC/BCOC staff with NBC expertise.
- Provide NBC defense support.
- Provide tenant-sector or base NBC emergency response teams (ERT) and support (e.g., NBC survey and monitoring teams, NBC casualty collection points, contamination control teams (CCTs), MOPP exchange points, and medical CB incident response teams/emergency medical teams).[32]

With the OPLAN approved, staff officers then convert the plan into an effective OPORD for crisis planning/execution. Critical staff tasks involve follow-up and supervision to ensure mission support resources are deployed and synchronized to execute successfully the NBC tasks identi-

fied in the OPLAN. Periodic reassessments of the JIPB, facts, assumptions, and "details" such as unit/resource availability provide necessary updates for improving the NBC defense annex to the OPORD.[33]

Operational planners track and maintain asset availability and visibility during planning, deployment, and execution. Resourcing begins during COA development by recommending the best combination of resources to support the mission and COA. As the situation develops, planners identify required functions and recommendations for the time-phased force deployment list (TPFDL) emerge. These recommendations should heed basic resource considerations and should not be restricted by current task organization. Basic resource considerations include mission requirements, resource capabilities, and resource availability/visibility.[34]

Primary sources of NBC defense assets include DOD units and NBC defense equipment. Functionally, NBC defense equipment can be classified IAW the NBC defense principles: avoidance, protection, and decontamination. Since thorough decontamination requirements may exceed support capabilities, the commander aggressively manages and prioritizes these decontamination assets. Additionally, fixed site NBC defense resource needs may require international/coalition or HN support. Appendix B of FM 3-11.34 (3-4-1) provides detailed resourcing information and options for use during planning. It addresses capabilities useful for fixed site NBC defense. However, it does not address all the specialized variations of some NBC defense equipment, (i.e. variations of aircraft protective masks). Table III-2 within that manual provides an example operational status chart for fixed site commanders to track NBC defense requirements.[35]

EXECUTION CONSIDERATIONS FOR NBC DEFENSE

The execution of NBC defense operations consists of sensing nuclear, biological, and chemical hazards—including toxic industrial materials—resulting from symmetrical and asymmetrical attacks on friendly formations, key infrastructure, and lines of communication; shielding the force by reducing the threat, reducing friendly vulnerability, and avoiding NBC hazards. Execution also includes sustaining the force by restoring combat power, critical infrastructure, and freedom of maneuver; and shaping the battlefield through NBC battle management.[36]

All units in the Army and joint rear areas actively participate in the planning and execution of NBC defense operations. Only through a coordinated effort in which all units—not solely specialized chemical units—perform defensive measures can the ASCC's critical functions continue to be performed effectively. The performance of allocated defensive tasks counters the effects, including cumulative effects, of employing NBC weapons. However, they make normal opera-

tions more difficult and reduce overall efficiency; therefore, the affected commander must consider mission degradation and hazards when employing defensive measures. Defensive tasks include contamination avoidance, protection, and decontamination. See FM 3-11.3 (3-3), FM 3-11.4 (3-4), *NBC Protection.*[37]

While each Service has the responsibility for NBC defense, greater effectiveness may be realized through cross-service operating agreements either at DOD or theater level. When cross servicing applies, the Army normally supports the other services. For example, the Army will normally provide NBC units for protection of the JRA.[38]

NBC Reconnaissance Companies, Dual-purpose Reconnaissance/Decontamination Companies, and Bio-Detection Companies when assigned to the theater chemical brigade conduct NBC reconnaissance and surveillance missions in the COMMZ and JRA to sense NBC hazards and shield friendly forces. The commander employs his NBC Reconnaissance and Bio-Detection units near airports of debarkation (APOD), seaports of debarkation (SPOD), logistical and maintenance facilities, critical routes, and rear operations centers (ROC) to support reception, sustaining, and command and control operations. NBC reconnaissance units report information to the NBC centers (NBCC). The NBCC analyzes the information and disseminates it through appropriate NBC reports to US and multinational forces.[39]

NBC Reconnaissance Companies and Dual-purpose NBC Reconnaissance/Decontamination Companies employ the M93 series Nuclear, Biological, and Chemical Reconnaissance System (NBCRS), a lightly armored vehicle equipped with a mobile mass spectrometer (MM-1), a remote sensing chemical agent alarm (RSCAAL), and a radiac meter. These systems enable the NBCRS crew to conduct nuclear and chemical route, area, and zone reconnaissance as well as to conduct surveillance on chemical named areas of interest (NAI) up to five kilometers away (line of sight).[40]

Bio-Detection Companies conduct biological surveillance in the COMMZ and JRA utilizing the M31 series Biological Integrated Detection System (BIDS) and the helicopter mounted Long-Range Standoff Biological Detection System (LRSBDS). The BIDS is a point detector mounted on a High Mobility Multi-purpose Wheeled Vehicle (HMMWV). These systems provide a basis for medical personnel to determine effective preventive measures and appropriate treatment if exposure occurs. Detection and identification of biological agents within the AO will limit adverse effects on operations and sustaining systems. See FM 3-11.86 (3-101-6), *Biological Defense Operations Corps/Company Tactics, Techniques, and Procedures.*[41]

Decontamination and Dual-purpose Smoke/Decontamination Companies assigned to the theater chemical brigade conduct mobile terrain, fixed site, and sustained thorough decontami-

nation missions in the COMMZ and JRA to sustain the force by restoring combat power, critical infrastructure, and freedom of maneuver. Decontamination units employed near APODs, SPODs, logistical and maintenance facilities, critical routes, and rear operations centers (ROC) to support reception, sustaining, and command and control operations.[42]

The transition to conflict termination must include a comprehensive effort to locate, identify, secure, and recover residual adversary NBC capabilities. This effort may have begun during hostilities. However, if friendly forces have not captured adversary NBC weapons and facilities during the campaign, gaining control of them before cessation of hostilities is likely only if the adversary has collapsed to the point where cease-fire terms can be dictated. Completion of search, identification, control, and recovery tasks provides a critical foundation for post-conflict planning to eliminate adversary capabilities and establish effective monitoring and other controls.[43]

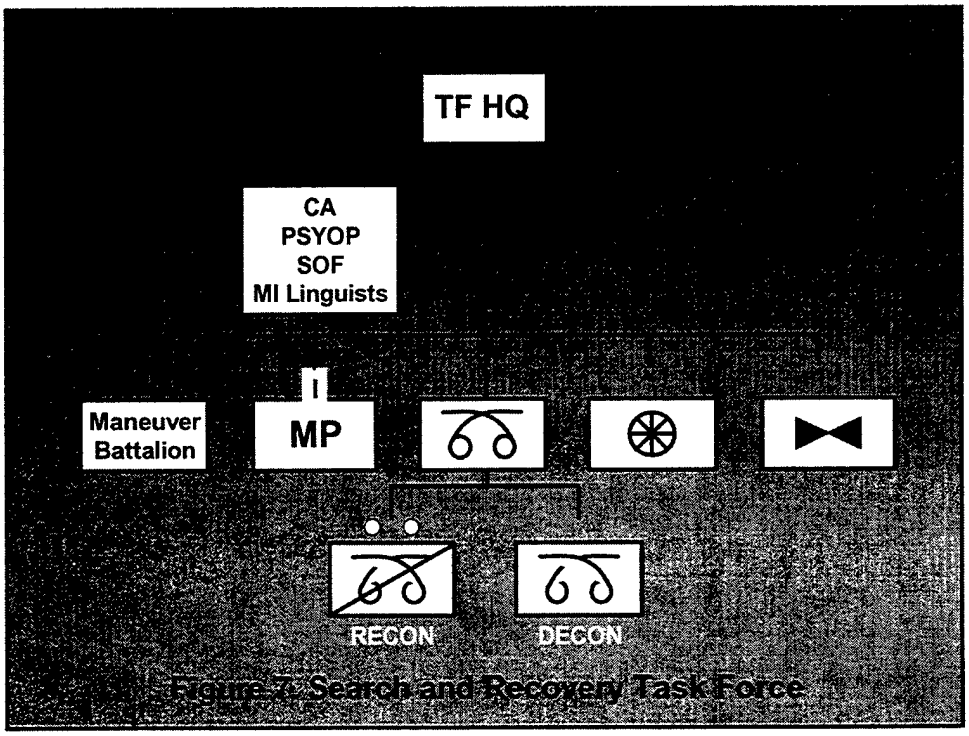


Figure 7. Search and Recovery Task Force

A recovery, search, identification, and control plan should be established and executed with sufficient forces to gain timely control of NBC capabilities. Specifically designated search and recovery task forces (S/RTFs), normally provided from the ARFOR, should be responsible to the JFC and include personnel with the technical proficiency necessary to identify and evaluate NBC weapons, equipment, and associated materiel. Figure 7 depicts a notional Army S/RTF organization. S/RTFs should also be capable of emergency response to NBC accidents or incidents. S/RTFs should be prepared to initiate operations as soon as a cease-fire is in effect or, at the latest, upon the formal cessation of hostilities. Assuming ongoing efforts by the adversary to disperse, conceal, or remove NBC capabilities, early expansion of the area un-

der positive US and multinational control is a central concern. See JP 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments.*[44]

The JFC must determine the appropriate mix of forces to accomplish NBC-related conflict termination objectives. Security and compliance forces, such as ARFOR combat, military police, and engineers will be needed in addition to specialized intelligence, technical, and medical personnel. ARSOF may also be required to perform civil-military operations (CMO) and civil affairs activities, and PSYOP tasks specifically related to NBC aspects of conflict termination.[45]

In the early stages of post-conflict operations, returning US equipment to CONUS or other locations will be a major activity as forces withdraw from the theater of operations. Goals for contaminated materiel retrograde from the theater are mission support, protection of forces and resources from NBC hazards, and the control of contamination. The JFC will establish the relative priority among these goals in view of the circumstances at hand, in particular operational timing and the extent of contamination. The safety of service members and transport personnel is of foremost concern during the CONUS retrograde of equipment with potential residual or low-level NBC contamination. The Army developed procedures to protect personnel against low-level NBC exposure resulting from maintenance or transportation actions, conserve valuable assets, and maintain DOD life cycle control of previously contaminated equipment. With current decontamination technology constraints, some equipment may require extensive weathering to meet safety objectives, and in some cases, equipment may require destruction. Generally, civil aircraft are not used to transport equipment with residual NBC contamination due to safety and legal concerns. Additionally, execution of these procedures will require extensive support from subject matter experts, government agencies, and senior leadership. See FM 3-11.34 (100-17-5) for additional redeployment considerations.[46]

ANTITERRORISM

Every commander, regardless of echelon of command or branch of Service, has an inherent responsibility for planning, resourcing, training, exercising, and executing antiterrorism measures to provide for the security of the command. Likewise, every military Service member, Department of Defense (DOD) employee, DOD independent contractor, and local national hired by the Department of Defense, regardless of rank, has an inherent responsibility to maintain vigilance for possible terrorist actions and to ensure that, where applicable, family members understand and employ antiterrorism tactics, techniques, and procedures. Specific DOD offices and agencies have been assigned specific responsibilities pertaining to combating terrorism.[47]

The Department of Defense is not the lead agency for combating terrorism. The Department of Defense is responsible for protecting its own personnel, bases, ships, deployed forces, equipment, and installations. The Department of Defense is also responsible for providing technical assistance or forces when requested by the National Command Authorities. The lead agency is the Department of State for incidents outside the United States, the Department of Justice for incidents within the United States, and the Department of Transportation and/or Federal Aviation Administration for certain aviation incidents.[48]

Joint doctrine defines antiterrorism as defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces.[49] Antiterrorism programs form the foundation for effectively combating terrorism. The basics of such programs include training and defensive measures that strike a balance among the protection desired, the mission, infrastructure, and available manpower and resources.[50]

The Army force commander's antiterrorism program concept is an integrated, comprehensive approach within the theater to counter the terrorist threat to military installations, bases, facilities, equipment, and personnel. The concept has two phases—proactive and reactive. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident.[51]

Counterterrorism (CT) is a highly specialized, resource intensive mission. Certain special operations forces units maintain a high state of readiness to conduct CT operations and possess a full range of CT capabilities. Each combatant commander maintains designated CT contingency forces within his Joint Special Operations Task Force (JSOTF) to respond to CT situations occurring within his area of responsibility when national assets are not immediately available. The combatant commander can place these CT assets in support of the Army force commander when required by the factors of METT-TC. However, it is more likely that the Army force commander will provide support to theater or national CT elements operating within his area of operations. In this case, there will be a Joint Special Operating Area (JSOA) designated.[52]

Terrorism is a major factor across the range of military operations. In the context of peacetime military operations, terrorism attracts a great deal of attention and few question its actual and potential capacity to kill and destroy. The same can be said of terrorism as an aspect of military operations other than war (MOOTW); however, in war the threat of terrorism is only one of many force protection issues the commander must consider. The same types of acts that

gain attention in peacetime military operations can hinder military operations in war (e.g., espionage, sabotage, vandalism, or theft).[53]

All acts of violence against the US military are not necessarily terrorist actions (e.g., murder or robbery). The measures contained within this publication provide guidance that will help protect the military unit and Service member from these acts of violence as well as those committed by terrorists. In peacetime military operations, there is no definitive method of differentiating terrorist acts from other violent crimes because the perpetrator's intent may be the only discriminator. A rule of thumb that can be applied is if the act is obviously related to personal gain (robbery of money or high-value items) or personal motivation (hatred, love, revenge) it is a crime, but probably not terrorist-related. On the other hand, if the act appears to adversely affect military operations (communications facilities, fuel storage areas) or has a high symbolic value (headquarters, particular individuals), the crime probably has terrorist implications even when no claim is forthcoming. Recognizing the difference between acts of violence and terrorist acts is vital in order to properly understand the threat's intent and determine required defensive measures.[54]

ORGANIZATION OF FORCES

The command responsibilities outline in Appendix E of FM 3-90 for rear area and base security also apply to the conduct of antiterrorism operations within a theater of operations. Each echelon of command forms a preventive AT planning organization. The planning organization is normally composed of individuals from the echelon, base cluster, or base operations center during crisis management, as well as additional staff representation from special offices such as the budget or civilian personnel offices. The planning organization will establish a threat committee to assess current threat information. These individuals are responsible for the security and protection of the echelon, base cluster, base, or installation from terrorist actions. The preventive planning organization should include staff from operations, intelligence, counterintelligence, law enforcement and/or security forces, engineers, legal, public affairs, and NBC representatives. This organization should consider the unit, base cluster, or base's defenses from an AT perspective to assess the terrorist threat. It integrates the unit, base cluster, or base's physical features with its security force capabilities, develops plans to compensate for weaknesses, and recommend enhancements (including education and awareness programs) that reduce the unit, base cluster, or base's vulnerabilities. The threat committee improves its parent organization's capabilities for detection and assessment.[55]

Units who are not under the control of a base cluster or base commander but are assigned or attached to the installation are tenant commanders. If all forces are from the Army, then Army rear area and base security doctrine found in FM 3-90 will apply. If the installation has tenants from more than one service, the provisions of Joint Pub 3-10, "*Doctrine for Joint Rear Area Operations,*" Chapter II, Paragraph 3b apply. Tenant commanders are still responsible for their command's physical security and for terrorism planning not provided by the installation or base commander. If the forces concerned meet the definition of transient forces, the provisions of Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)," Chapter IV, Paragraph 1b apply.

CONTROL MEASURES

Control measures in antiterrorism operations are the same as those used in other defensive operations. (See Figure 8.) The headquarters establishing the base or base cluster designates the base's AO using rear, lateral, and forward boundaries. The AO for the base may or may not be contiguous to the AO of other units. The echelon rear area commander may further subdivide his assigned area into subordinate AOs, bases, and base clusters. He can assign maneuver forces to assembly areas and battle positions. He establishes phase lines, contact points, objectives, and checkpoints as necessary to control his maneuver. He establishes fire support coordinating measures (FSCM) to permit or restrict fires in and around the base. (See FMs 3-90 and 3-09 (6-20) for a discussion of FSCMs.) No-fire areas may be required to protect civilians, prevent disruption of sustaining operations, or protect combat outposts, observation posts, and patrols from friendly fire. All established control graphics are coordinated with host nation agencies to minimize interference, misunderstandings, and unnecessary collateral dam-

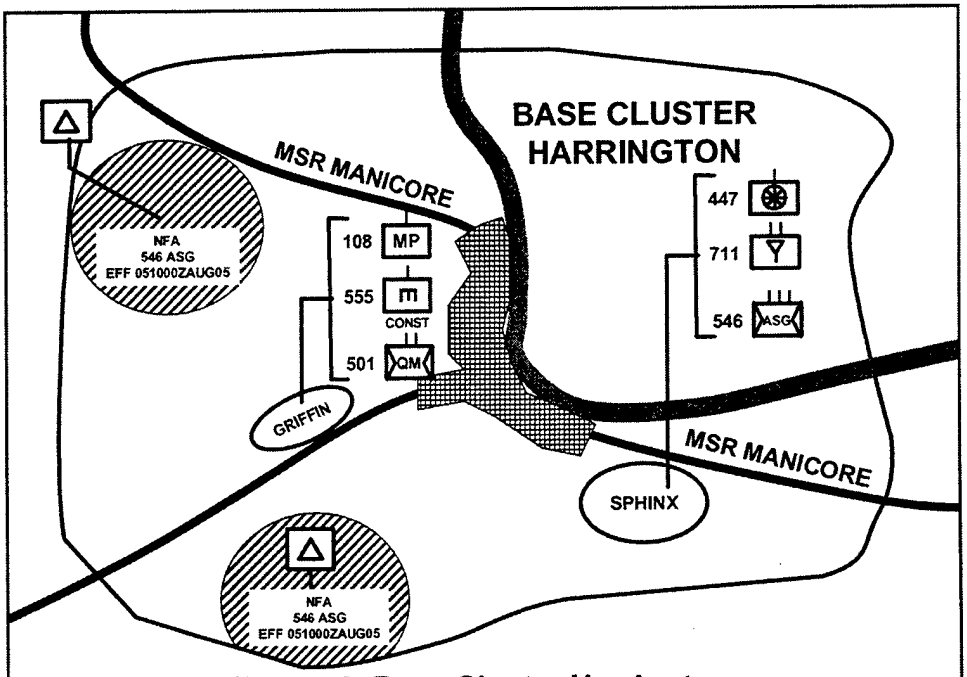


Figure 8. Base Cluster Harrington

age. The Base Defense Force commander, in coordination with the base commander, designates the base perimeter, target reference points, and sectors of fire to organizations located within the base.

ANTITERRORISM PLANNING

The Army force commander designates a staff office within his headquarters, usually from the G-3 Operations or Provost Marshall Office, to supervise, inspect, test, and report on the base AT programs within the theater. This office also coordinates with host-nation authorities through the G-5 and US embassies. Simultaneously, the G-2 disseminates intelligence on terrorist activities to the subordinate commands to ensure that the AT measures are appropriate to the threat. The manner in which the Army force commander places importance on these staff functions usually has a direct affect on the AT readiness of subordinate commands.[56] This process repeats down the chain of command to the base cluster and base.

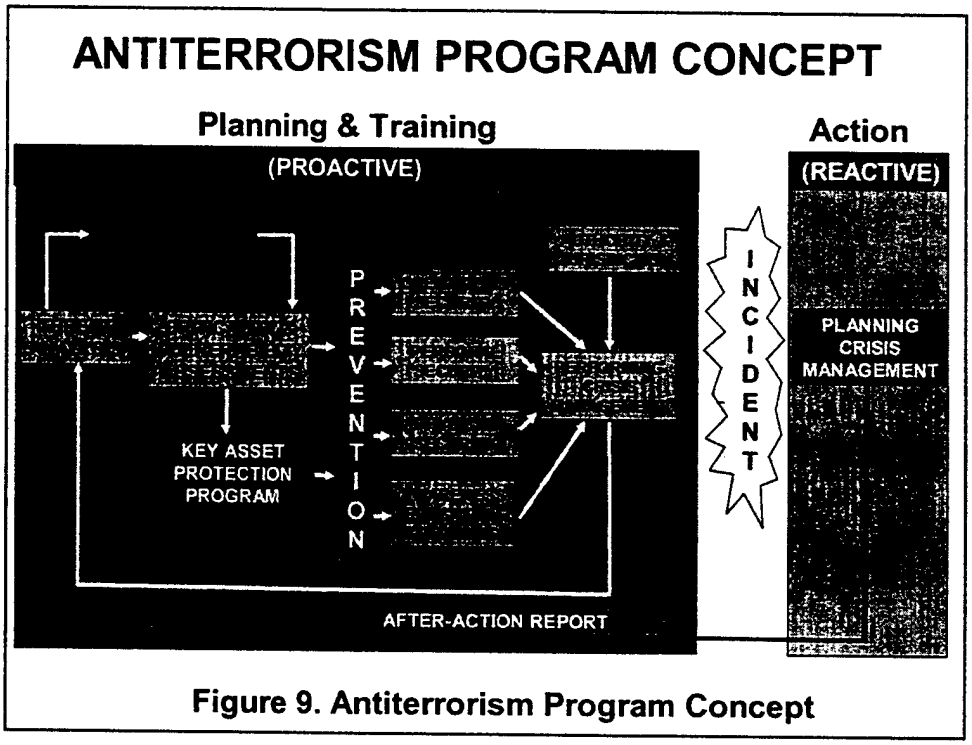


Figure 9. Antiterrorism Program Concept

The AT program stresses deterrence of terrorist incidents through preventive measures common to all Army units. (See Figure 9.) The program addresses:

- Threat analysis;
- Installation or unit criticality and vulnerability assessments;
- Creation of a threat assessment based on the threat analysis and friendly vulnerabilities;
- Information security;
- OPSEC;
- Personnel security;
- Physical security;

- Crisis management planning;
- Employment of tactical measures to contain or resolve terrorist incidents;
- Continuous training and education of personnel; and
- Public affairs planning.[57]

See Chapter 4 of JP 3-07.2 for a detailed explanation of these program elements.

The commander and staff should complete a thorough security estimate of the situation using the factors of METT-TC as a guide for developing the assessment. The following questions aid in developing an estimate of the terrorist situation:

- Mission: (1) Who is being tasked? (2) What is the task? (3) When and where is this task to take place? (4) Why are we performing this task?
- Enemy: (1) Who are the potential terrorists? (2) What is known about the terrorists? (3) How do the terrorists receive information? (4) How might the terrorists attack? (Think like the terrorists! Would you ambush or raid? Would you use snipers, mortars, rockets, air or ground attacks, suicide attacks, firebombs, or bicycle, car, or truck bombs?) (5) Does your unit have routines? (6) What is the potential for civil disturbances and could terrorists use or influence these disturbances in an attack? Local law enforcement personnel (e.g., host-nation police) can at times be a valuable source for this information.
- Terrain and weather: (1) What are the strengths and weaknesses of the installation, base, ship, port, and local surroundings? (2) Are the avenues of approach above or below the water or ground? (3) Are there observation areas, dead spaces, fields of fire, illumination, or no-fire areas (e.g., schools)? (4) Are there tall buildings, water towers, or terrain either exterior or adjacent to the perimeter that could become critical terrain in the event of an attack?
- Troops and support available: (1) Determine what is the friendly situation. (2) Are other US forces or equipment available? (3) Are engineers and/or EOD in the area? Will they be able to provide support? (4) Are emergency reinforcements available? (5) Are MWD teams available? (6) What are the host-nation responsibilities, capabilities, and attitudes toward providing assistance? (7) What restraints will be imposed by the US Government on the show or use of force?
- Time available: (1) What is the duration of the mission? (2) Are there time constraints? (3) Will there be sufficient time to construct force protection facilities such as barriers, fences, and lights?
- Civil Considerations: (1) Are there host-nation concerns or attitudes that will impact on the situation? (2) Will the situation be influenced by the existence of any religious or racial concerns?[58]

The AT defensive plan should include a combination of law enforcement and security assets, fortifications, sensors, obstacles, local-hire security forces (if applicable), unit guards, deception, and on-call support from reaction forces. Each situation requires its own combination of abilities based on available resources and perceived need.[59]

ANTITERRORISM PREPARATIONS

The mechanism by which the AT program operationally increases or decreases protective measures for bases and installations is the DOD THREATCON System. (See Appendix J, THREATCON System, of JP 3-07.2.) As a DOD-approved system, the terms, definitions, and prescribed security measures facilitate inter-service coordination, reporting, and support of US military AT activities. Selection of the appropriate response to terrorist threats remains the responsibility of the commander having jurisdiction or control over threatened facilities or personnel.[60]

Military units and individual service members within a theater of operations should take preventive and protective security measures to protect themselves and their ability to accomplish their mission during deployment and expeditionary operations. Additionally, rest and recuperation (R&R) facilities require close consideration. These facilities are frequently vulnerable due to their location and generally easy access. Service personnel are at risk of lowering their guard while using these R&R facilities. The base, port, or installation AT plan provides the mechanism to ensure readiness against terrorist attacks while the unit performs its tactical and technical missions. The degree of the protection required depends on the threat in a given location.

Measures taken to establish the defense must be continually reviewed and progressively updated to counter the changing threat and add an element of unpredictability to the terrorist's calculation. This responsibility cannot be ignored in any situation. Local security must be around-the-clock to provide observation, early warning and, if necessary, live fire capabilities.

ANTITERRORISM EXECUTION

The response to a terrorist incident varies depending on the nature and location of the incident. Recognizing that many incidents do not develop beyond the first phase, there are generally three distinct phases through which an incident may evolve.[61]

Phase I is the commitment of locally available resources. This includes available military law enforcement personnel, security force patrols or guards, and available backup units. Ideally, all law enforcement or security personnel are familiar with local SOPs for terrorist incidents and practice these procedures as part of their unit-training program. They must be prepared to secure, contain, and gather information at the scene until the beginning of Phase II. Because terrorist incidents often include diversionary tactics, response forces must be alert to this fact while securing and containing the incident scene. The evacuation of threatened areas is a priority function.[62]

Phase II is the augmentation of the initial response force by additional law enforcement and security personnel and/or a specially trained response force—special reaction team, emergency services team, FBI regional special weapons and tactics units or the hostage rescue teams, or host-nation tactical units. This phase begins on activation of the operations center. During this phase, either the FBI or the host nation may assume jurisdiction over the incident. If that occurs, military forces must be ready to support the operation. The installation, base, ship, unit, or port specially trained reaction force must be ready for employment in this phase of the operation. In any country in which a terrorist incident against an American facility or unit occurs, the DOS and the US Embassy will play the key role in coordinating the US Government and host country response to such an incident.[63]

Phase III is the commitment of the specialized FBI, DOD, or host-nation counterterrorist force. This is the phase in which steps are taken to terminate the incident. Incident termination may be the result of successful negotiations, assault, or other actions including terrorist surrender. Because identifying the terrorists, as opposed to the hostages, may be difficult, capturing forces must handle and secure all initial captives as possible terrorists.[64]

Those antiterrorism guard, patrolling, road movement, vehicle protection, and convoy, rail, sea, and air movement considerations outlined in Chapter 7 of JP 3-07.2 apply to those tactical activities performed by subordinate elements within the theater.

DEFENSIVE INFORMATION OPERATIONS

Information operations are actions taken to affect adversary, and influence others', decision-making processes, information and information systems while protecting one's own, information and information systems. Commanders use offensive IO and defensive IO simultaneously or sequentially to increase their forces' effectiveness and protect their organizations and systems. IO are executed through a combination of these elements, discussed in detail in Chapter 2 of FM 3-13 (100-6), *Information Operations*—

- Operations Security (OPSEC).
- Psychological Operations (PSYOP).
- Counterpropaganda.
- Military deception.
- Counterdeception.
- Electronic Warfare.
- Computer network attack (CNA).
- Physical destruction.
- Information assurance.
- Physical security.

- Counterintelligence.
- Special IO.

Activities that may contribute to IO are Public Affairs and Civil Military Operations. Information operations are shaping operations that create and present opportunities for decisive operations. Information operations are both offensive and defensive.[65]

Defensive information operations (IO) are the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly, information and information systems. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Defensive IO means range from nontechnical techniques and procedures, such as OPSEC, to technical techniques and procedures, such as information assurance.[66]

Operational level commanders depend on the information provided by their command and control systems to plan their operations, deploy forces, and execute assigned missions. The information systems found within their command posts serve as enablers and enhance their warfighting capabilities; however, increasing dependence upon rapidly evolving technologies makes their forces more vulnerable. Since it is a practical impossibility to defend every aspect of our infrastructure and every information process, defensive IO ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives. Four interrelated processes comprise defensive IO: information environment protection, attack detection, capability restoration, and attack response. Offensive actions play an integral role in the defensive process in that they can deter adversary intent to employ IO and/or neutralize adversary capabilities. The defensive IO processes integrate all available capabilities to ensure defense in depth. This includes the full integration of the offensive and defensive components of IO.[67]

The primary IO elements used to conduct defensive IO are counterdeception, counter-propaganda and information assurance (IA). Counterdeception and counter-propaganda aid protecting the decision maker and the friendly forces. Information assurance protects and defends against enemy actions to ensure availability, integrity, authentication, confidentiality, and nonrepudiation of friendly information and information systems.

- Availability. Timely, reliable access to data and services by authorized users. Available INFOSYS operate when needed.
- Integrity. Protection from unauthorized change, including destruction. INFOSYS with integrity operate correctly, consistently, and accurately.

- Authentication. Certainty of user or receiver identification and authorization to receive specific categories of information.
- Confidentiality. Protection from unauthorized disclosure.
- Nonrepudiation. Proof of message receipt and sender identification, so neither can deny having processed the data.[68]

ORGANIZATION OF FORCES

The operational-level commander has an operational level information operations (IO) cell within his headquarters to coordinate and deconflict the separate IO elements that support his ongoing and future campaigns and major operations. This cell is responsible for planning how the command will achieve and exploit information superiority. The nucleus of the IO cell is the echelon IO section. Each echelon IO cell includes representatives of special and coordinating staff sections as the mission requires. The echelon assistant chief of staff G7, Information Operations Coordinator (IOCOORD) is responsible for the activities of the IO cell and chairs the IO cell meetings. At the ASCC, coordination of IO is done between the current operations division, plans division, and the effects control divisions of DCSOPS.[69]

The IOCOORD is the principal staff officer for all matter concerning information operations. The IOCOORD, a FA 30 officer, reports to the chief of staff on the status of achieving information superiority. The IOCOORD ensures the execution of information operations for the commander. He ensures the accomplishment of echelon IO actions. The following are the IOCOORD's specific responsibilities:

- Supervises the IO Section.
- He synchronizes and coordinates offensive and defensive IO.
- Assess impact of offensive IO and defensive IO.
- He integrates intelligence from the G2 into IO.
- Establish priorities to accomplish IO tasks from the MDMP.
- Provide input into the CCIR process.
- Coordinates and synchronize IO at the theater strategic, operational, and tactical and in Army, Joint, and Multinational operations.
- Coordinate information operations across the staff.
- Synchronize IO effects to influence adversary perceptions, decisions, and actions.
- Responsible for the overall planning, preparation, execution and assessment of information operations.
- Writes the IO annex.
- Synchronizing the capabilities of the IO section, leveraging the capabilities of higher echelon IO agencies and units providing connectivity with national-and theater-level IO agencies and monitoring the execution of the elements of IO to ensure the delivery of massed information effects when needed.[70]

Figure 10 shows the make up of an example IO cell. Appendix F of FM 3-13 (100-6), *Information Operations,* details the information operations related duties of each of the individuals depicted in the figure. The IO cell may conduct coordination in a formal coordinating meeting. In a less formal setting, the IO cell coordination may take place by communicating over the local area network with IO section personnel. The frequency and times of IO cell meetings are synchronized with the command's battle rhythm.[71]

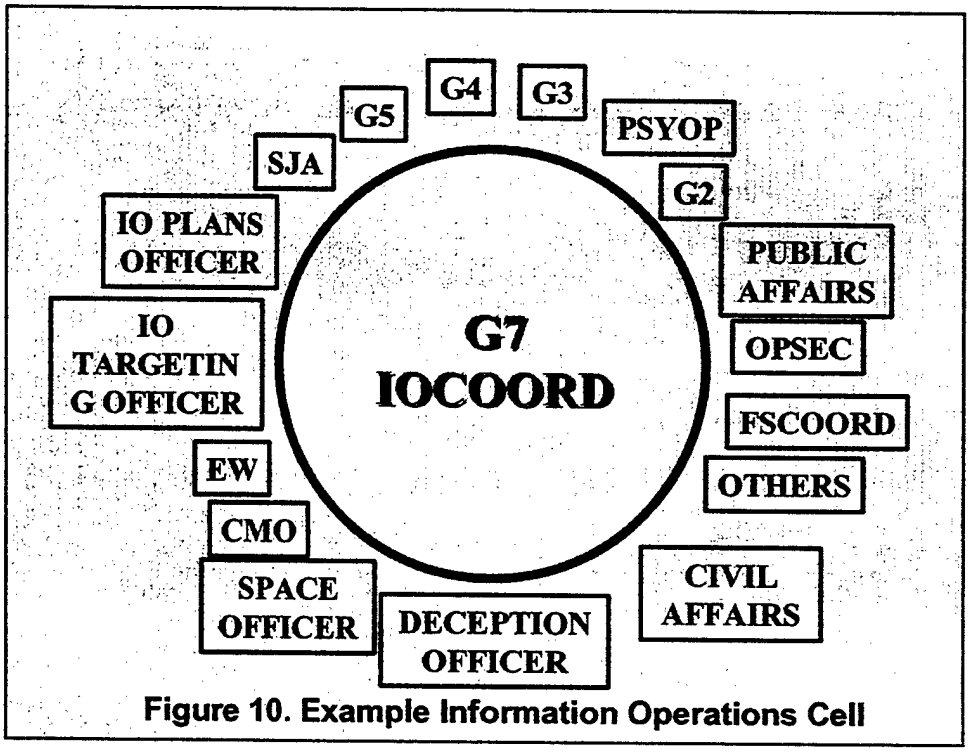


Figure 10. Example Information Operations Cell

The IO cell provides recommendations to the echelon chief of staff and input to the targeting process. It coordinates with the next higher echelon to ensure its IO objectives are met and with subordinate echelons to ensure the IO objectives of the commander are included in the subordinate's plans as required. In the targeting process the output of the IO cell meeting is input to the command's targeting cell meeting.[72]

When requested, a Field Operations Team (FST) from the Army's Land Information Warfare Activity (LIWA) can augment the operational commander's IO section. The FST will assist the IOCOORD and coordinate with the Joint Information Operations Center (JIOC). They provide input to the IOCOORD for the IO Annex. Specific IO duties of a FST include—

- Coordinate computer emergency response team (CERT) operations to the command.
- Coordinate Army reprogramming analysis team–threat analysis operations to the command.
- Coordinate with the special technical operations (STO) representative for the IOCOORD for specific STOs.
- Coordinate vulnerability assessment operations to the command.
- Provide connectivity to national-level IO databases.

See Appendix B of FM 3-13 (100-6) for detailed discussion of LIWA.[73]

The OPLAN/OPORD task organization shows the organization for combat of the command, including assigned and attached units with IO capabilities. This organization coupled with the known status of the task-organized units identifies the capabilities and limitations of the command. IO assets can be derived from the OPLAN/OPORD task organization paragraph or annex, the Intelligence annex as well as the IO-specific annexes. The Fire Support annex also identifies assets that may support IO with physical destruction. The Air Tasking Order shows the availability of joint air assets that can support Army IO.[74]

CONTROL MEASURES

There are no control measures unique to defensive information operations. A commander employs fire support coordinating measures (FSCM) outlined in FM 3-90 and FM 3-09 (6-20) as appropriate.

PLANNING CONSIDERATIONS

As with the other elements of combat power, there is no universal formula for the application of information operations. The factors of METT-TC determine the IO tactics, techniques, and procedures (TTP) and the combination and method of IO element employment for any given environment. For example, in operational-level offensive operations, the elements of physical destruction, EW, and military deception may predominate with support provided by OPSEC, PSYOP, CMO, and PA. In operational-level stability operations, IO may focus primarily on PSYOP, supported by CMO, and PA.[75]

By using the military decision-making process (MDMP) and supporting intelligence preparation of the battlefield (IPB) and the targeting processes, the echelon IO staff develops a plan, in the form of an IO annex to an OPLAN/OPORD, which considers all of IO's capabilities and synchronizes them as appropriate into the operation.[76]

Information operations planning takes place within the MDMP, as described in FM 5-0 (101-5). The MDMP aids the IO staff to develop a viable IO estimate and an effective IO concept of support for the command's planned operation. Appendix B of FM 3-13 (100-6) provides an example of an IO estimate. Using the MDMP as a common planning tool ensures the full synchronization of IO and its diverse elements into the echelon's full-spectrum operations.[77]

Field Manual 3-13 (100-6) provides planning techniques designed to ensure the integral integration of IO into the overall operations planning effort within the structure of the MDMP. (See Figure 11.) They prevent the conduct of IO as a separate, stovepipe process. This methodology allows the IO staff to develop objectives, tasks, and appropriate input that staff planners

will immediately recognize and synchronize into their planning processes, making the IO staff full participants in the command's overall operations planning effort.[78]

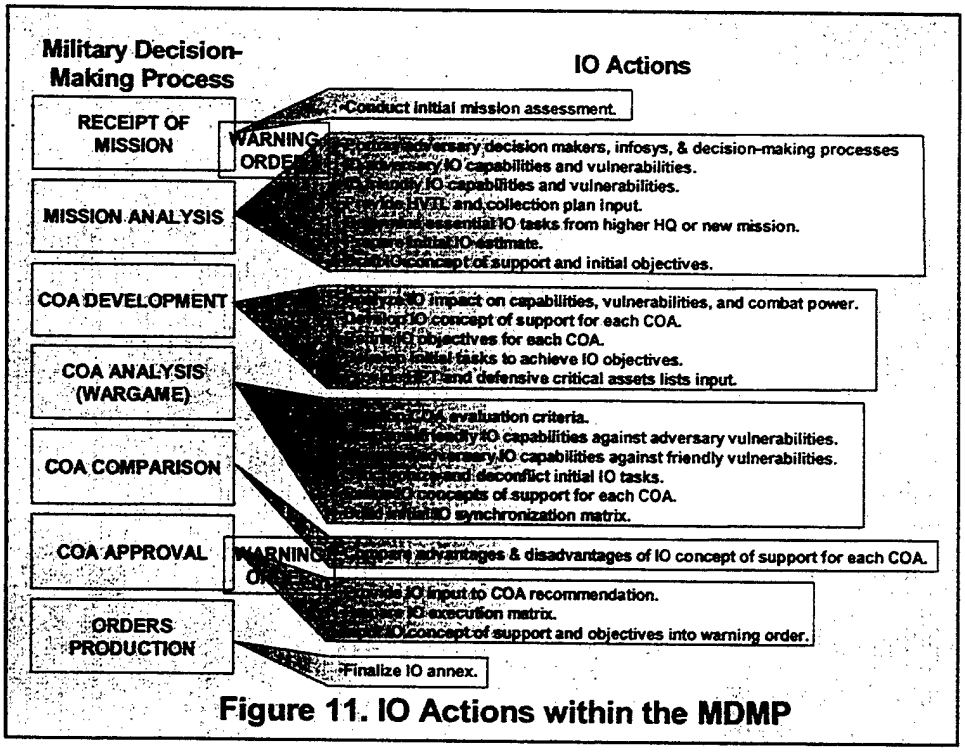


Figure 11. IO Actions within the MDMP

The commander's personal interest and involvement is essential to ensure IO effectively supports the mission. To achieve this, the commander and staff planners consider IO throughout the planning process, from receipt of a mission to course of action approval. Additionally, two other key planning processes that supports the MDMP consider IO—intelligence preparation of the battlefield (IPB) and targeting. (See FM 2-01.3 (34-130), *Intelligence Preparation of the Battlefield*, and FM 3-60 (6-20-10), *TTP for the Targeting Process.*) IPB supports IO by highlighting friendly and enemy IO capabilities and vulnerabilities. The targeting process integrates lethal and non-lethal attacks to support the operation, integrating IO into the target planning process.[79]

PREPARATION CONSIDERATIONS

During preparations, the operational commander establishes a protected information environment through development of common policies, procedures, and the incorporation of technological capabilities. This includes the inclusion of defensive IO objectives into operational plans and orders.

POLICIES

The Army operational commander augments standing defensive IO policies with joint force specific policies to provide integrated and focused information environment protection tailored to his specific OA. These policies should address vulnerabilities and threats, friendly force

capabilities, and commercial infrastructure dependencies and vulnerabilities that affect the various phases of an operation.[80]

PROCEDURES

Joint force procedures to implement the information environment protection policies should employ commonality to the greatest extent possible. Use of common procedures will help achieve secure interoperability between joint force components. Personnel security, industrial security, and physical security measures are examples of procedures contributing indirectly to information assurance.[81]

CAPABILITIES AND RELATED ACTIVITIES.

The following capabilities and related activities contribute to establishing the protected information environment. Operational forces conduct vulnerability analyses and assessments to identify vulnerabilities in their information systems and to provide an overall assessment of system security posture. Integrating vulnerability analysis capabilities into joint training, exercises, and modeling and simulations helps identify and mitigate vulnerabilities and directly contributes to information environment protection.

Foreign and internal threats are only a part of the overall threat to information systems. Internal threats from malicious, such as disgruntled workers, and accidental, such as magnetic emanations or electrical impulses, sources in addition to natural phenomena, such as sunspots, hurricanes, tornadoes, earthquakes, and floods, are significant concerns. Vulnerability analysis of systems must include consideration of these factors.

Vulnerability analysis and assessment efforts focus on specific types of information systems. For example, DISA operates a program known as the Vulnerability Analysis and Assessment Program specifically focusing on automated information systems (AIS) vulnerabilities. NSA has a communications security (COMSEC) monitoring program that focuses on telecommunications systems using wire and electronic communications.

Counterintelligence, personnel, physical, and facility security surveys are additional measures designed to determine and probe organizational IO vulnerabilities. Coordinated application of all these activities provides the organization a more complete vulnerability assessment and assists in risk management.[82]

The operational commander ensures the integration of information assurance capabilities to protect and defend information and information systems. He uses models and simulations to test these capabilities in joint exercises and Army training events. Supporting technologies include security measures such as information security (INFOSEC) devices.

INFOSEC is the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. INFOSEC is composed of computer security (COMPUSEC) and communications security (COMSEC). COMPUSEC involves the measures and controls ensuring confidentiality, integrity, and availability of information processed and stored by a computer. These include policies, procedures, and the hardware and software tools necessary to protect and defend computer systems and information. COMSEC includes measures taken to deny unauthorized persons information derived from telecommunications. COMSEC ensures telecommunications authenticity. COMSEC includes crypto-security, transmission security, emission security, and physical security of COMSEC materials and information.[83]

EXECUTION CONSIDERATIONS

Timely attack detection and reporting are the keys to initiating capability restoration and attack response. Determination and/or identification of adversary or potential adversary capabilities (such as EW and military deception) and their potential to affect friendly information and information systems play critical roles in capability restoration and attack response. Elements of IO attack detection include, but are not limited to, the following.[84]

Information Warfare Centers

The Service information warfare centers (Fleet Information Warfare Center, Air Force Information Warfare Center, and Land Information Warfare Activity) receive reports of CNA, issue warning reports, prepare and implement technical responses, coordinate restoration strategies, and prepare and issue analyses and reports.[85]

Information Systems Developers

Information systems developers help ensure systems, particularly automated information systems, are designed and fielded in a manner that mitigates potential technological, employment, or integration vulnerabilities. Automated information system design should include automatic detection, mitigation, and reporting mechanisms.[86]

Information Systems Providers and Systems Administrators

Increasingly powerful information systems attack techniques are continuing to emerge. Providers and administrators should recognize abnormalities in system functioning and be able

to take appropriate action to report and mitigate the effects of adversary actions. They also should establish a routine for periodic risk assessment and detection or mitigation system updates.[87]

Information and Information Systems Users

Users should be aware of potential threats to and vulnerabilities inherent in information systems. This includes recognizing abnormalities or unexplained changes in content or disturbed information and employing procedures for reporting incidents and safeguarding evidence.[88]

Law Enforcement

Operators and system administrators report intentional information systems incidents or intrusions to military criminal investigators and counterintelligence agents to coordinate appropriate action. The resulting investigations help support systems administrators, the intelligence community, systems developers, and, as necessary, the producers and users of affected information or information systems. Internal procedures should facilitate criminal or counterintelligence investigation of the incident while protecting the integrity of the information or information systems as well as protecting individual privacy rights.[89]

Intelligence

Intelligence contributes to attack detection by providing warning and assessment of potential adversary activity and cueing collection to specific activity indicators. Close coordination is required between intelligence, counterintelligence, law enforcement, systems developers, providers, administrators, and users to ensure timely sharing of relevant information.[90]

Indications and Warnings

Indications and warnings are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied/coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied/ coalition nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Indications and warnings for IO are provided by the National and DOD Warning Systems. Strategic I&W provide assessments of the level of threat posed by potential adversaries' IO-related activities.[91]

Defending against IO, whether it is an adversary's deception or propaganda, or IO conducted against a JFC's intelligence data base, an automated component of the commercial national power grid, or a satellite ground station, is predicated on how well the intelligence processes function and on the agility of systems providers, users, and administrators to implement protective countermeasures. In defensive IO, the strategic I&W process analyzes adversary intent, capabilities, history, opportunity, and targeting to assess the IO threat to provide sufficient warning to allow for actions to preempt, counter, or otherwise moderate their effect. (See Figure 12.)[92]

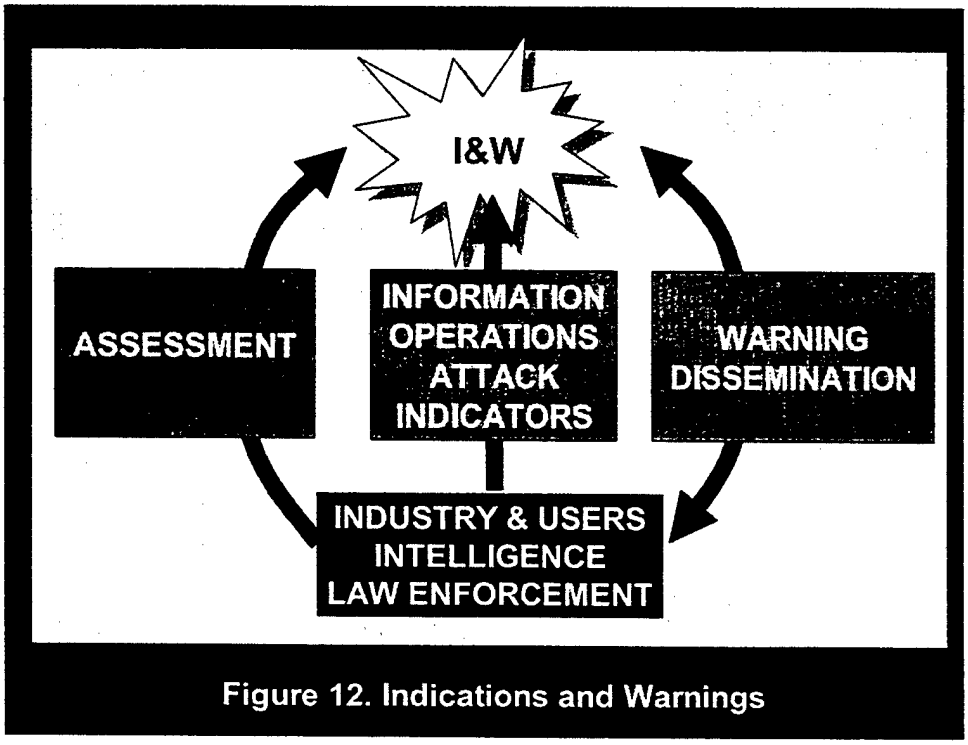


Figure 12. Indications and Warnings

Subordinate joint force indications and warning support to defensive IO relies on indicators from sources internal and external to the Department of Defense. Joint forces should continue to analyze traditional attack indicators until a comprehensive national I&W process is established that reflects the unique characteristics of IO. Traditional indicators include, but are not limited to, the following.

- Adversary or potential adversary capabilities.
- Adversary or potential adversary intentions, preparations, deployments and related activities, and possible methods of IO attack.
- Adversary motivations, goals, and objectives.
- Changes in adversary force dispositions, military and nonmilitary activities to conduct IO, and mobilization status.
- Required adversary mobilization preparations prior to military or nonmilitary IO taking place.[93]

Reporting Structure

Information systems designed to alert managers and administrators at all levels of abnormalities help contribute to attack detection. Timely collation, correlation, information analysis,. and warning dissemination require a continuously functioning reporting structure. A reporting structure linked to intelligence, counterintelligence, law enforcement, policy makers, and the information systems community, both government and commercial, is essential to defensive IO.[94]

Capability Restoration

Capability restoration relies on established procedures and mechanisms for prioritized restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer. Information system design and modification should consider incorporating automated restoration capabilities and other redundancy options. A collaborative effort among government, industry, and society is required (See Figure 13.)[95]

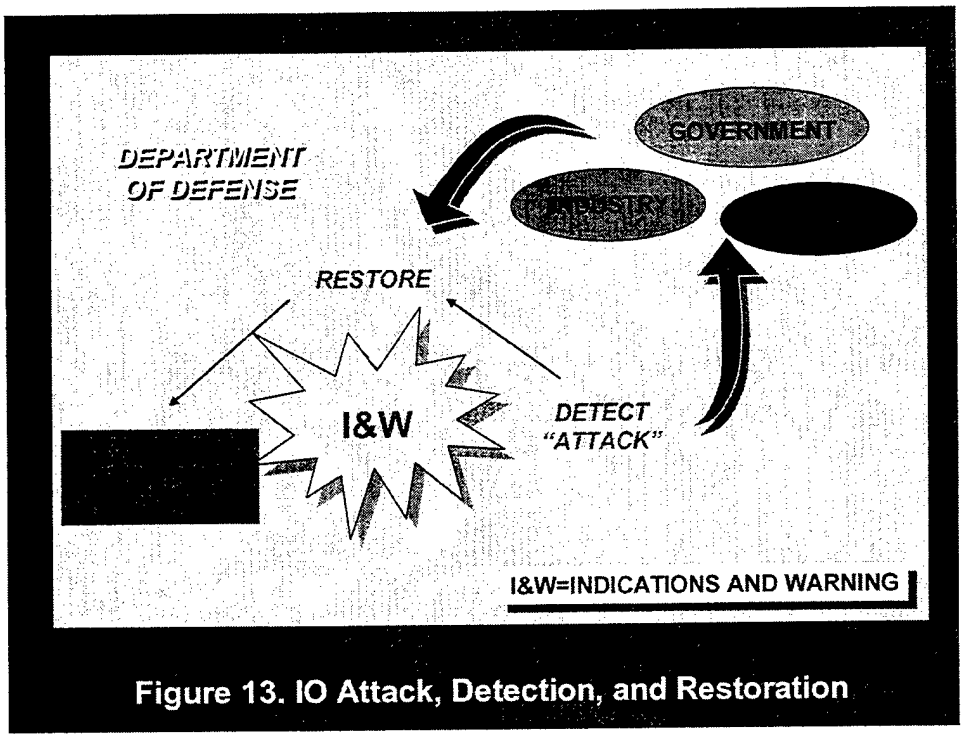


Figure 13. IO Attack, Detection, and Restoration

Computer Emergency Response Teams (CERTs)

CERTs are teams composed of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs for rapid response to deployed Service forces. Some combatant commanders have formed CERTs for similar response to subordinate joint forces within their combatant command AORs. In addition, Defense Information Systems Agency (DISA) can deploy CERTs to AORs or JOAs in response to specific requests for this capability. Service components submit

requests for CERTs from their own service through the administrative control line of authority. Requests for CERTs from DISA should be submitted through the supported combatant commander.[96]

Technical Restoration Capabilities

In some cases, required technical restoration capabilities are beyond the abilities of the affected sites. On-line or deployable restoration assistance capabilities can provide required expertise and tools to restore services. In addition to CERTs, there are security incident response centers. These capabilities exist at DISA and the Services and are available from commercial sources.[97]

Automated Intrusion Detection Systems

Automated intrusion detection systems provide managers and administrators with enhanced situational awareness and create decision points. Immediate termination of adversary information systems access to protect against further actions and information exploitation should be weighed against the needs of the law enforcement and intelligence communities to collect against and exploit the adversary. Information systems owners and/or designated approving authorities should seek higher authority approval before allowing an intruder to maintain access for purposes of gathering information to support IO response. The decision relies on a risk assessment of continued access, consideration of current and future operations, and intelligence impact.[98]

Inventory of Systems Resources

A key step in capability restoration is to inventory systems resources to help identify surreptitious adversary implants.[99]

Post-Attack Analysis

Post-attack analysis provides information about vulnerabilities exploited and leads to security improvements. Audit trails such as automated recording of specific attack techniques during the incident can provide information required for analysis.[100]

IO Attack or Potential Attack Response

IO attack detection or validation of a potential attack through analytical results of the I&W process trigger IO response. Timely identification of actors and their intent is the cornerstone of effective and properly focused response, thereby linking the analytic results of the I&W process

to appropriate decision makers. The JFC disseminates this information in a timely manner. (See Figure 14.)[101]

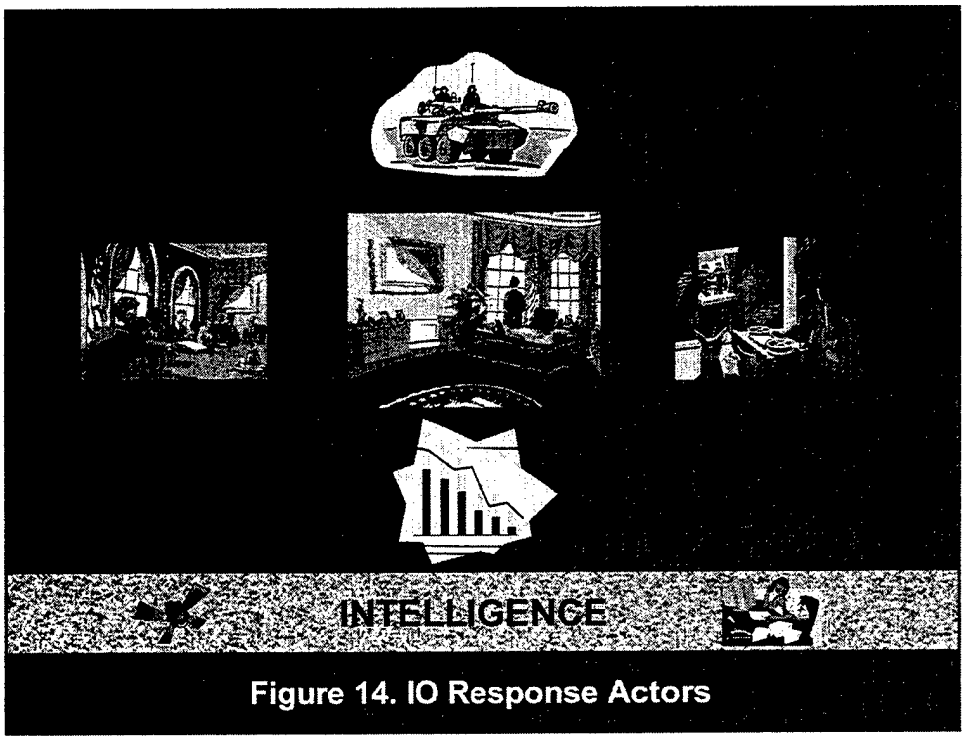


Figure 14. IO Response Actors

IO response involves identifying actors and their intent and establishing cause and complicity. It also may involve appropriate action(s) against perpetrators. The effectiveness of the IO response is dependent upon efficient integration of IO attack or potential attack detection and analysis capabilities. IO response contributes to defensive IO by countering threats and enhancing deterrence.[102]

Elements of the IO response may include national-strategic decisions to apply flexible deterrent options, either stand-alone or parallel. Possible response options include, but are not limited to, law enforcement, diplomatic actions, economic sanctions, and/or military force.[103]

Law Enforcement. Military and local law enforcement can contribute to information assurance by investigating information system incidents and intrusions and apprehending criminals. This may deter other criminals or adversaries. Law enforcement also provides investigative resources and maintains records on incidents, which may assist analysts in defining vulnerabilities.[104]

Diplomatic Actions. Diplomatic actions can provide a powerful deterrent without resorting to lethal force. Diplomatic actions can be taken at low cost, are scaleable, and are easily changed. Additionally, diplomatic actions can be taken by individual states or as a group.[105]

Military Force. Military force includes a range of lethal and/or nonlethal responses that may eliminate the threat directly or interrupt the means or systems that an adversary uses to conduct IO.[106]

Economic Sanctions. Economic sanctions offer another alternative to military force. Economic sanctions may weaken an adversary's position, thereby rendering him/her more

susceptible to other response options. Economic sanctions have a number of weaknesses, however, including enforcement, which often relies on military force.[107]

SECURITY TO OPERATIONAL FORCES AND MEANS

Security operations are those operations undertaken by a commander to provide early and accurate warning of enemy operations, to provide the force being protected with time and maneuver space within which to react to the enemy, and to develop the situation to allow the commander to effectively use the protected force. The ultimate goal of security operations is to protect the force from surprise and reduce the unknowns in any situation. A commander may conduct security operations to the front, flanks, or rear of his force. The main difference between security operations and reconnaissance operations is that security operations orient on the protected force or facility, while reconnaissance is enemy and terrain oriented. Security operations are shaping operations.[108]

Chapter 12 of FM 3-90 discusses security operations. Appendix E of FM 3-90 discusses rear area and base security. Those tactics and techniques are also valid to the conduct of operational-level protection. Specifically those tactics and techniques are applicable to the conduct of protection and security of operational flanks, rear areas, and lines of communications within a joint operational area. They also apply to the conduct of counterreconnaissance, the protection and security of operationally critical installations, facilities, and systems, and to the integration of host-nation security forces and means.

This section provides general guidance and links to specific tactics and techniques for two areas associated with the provision of protection to operational forces and means not elsewhere discussed in this manual—the preparation of operationally significant defenses and the removal of operationally significant hazards.

PRPARATION OF OPERATIONALLY SIGNIFICANT DEFENSES

Operationally significant defenses conserve the fighting potential of a force for application at the decisive time and place. Operational-level defenses include actions taken to counter the enemy's firepower and maneuver by making soldiers, systems, and operational formations difficult to detect, strike, and destroy. This includes—

- Effective use of camouflage and military deception on a large scale.
- Emplacement and construction of operationally significant barriers and obstacles.
- Incorporation of force-protection considerations into current and future engineer project designs.
- Conduct of geospatial analyses to assess the friendly force's vulnerabilities and the enemy's capabilities.[109]

Operationally significant defenses should significantly reduce the friendly troop strength required to occupy them—thus allowing the commander to reconstitute a significant offensive maneuver force. They should provide a significant increase in the defensive capabilities of friendly forces to allow them to repeal an enemy's attack. They should afford significantly greater protection to the forces occupying them. Ideally, they will provide all three advantages to the defender.

ORGANIZATION OF FORCES

An operational commander organizes his force to accomplish reconnaissance, security, main battle area, reserve, and sustaining operations. Chapter 9 of FM 3-90 explains the roles of each of these forces in detail.

The operational-level engineer forces discussed in FM 3-34.211 (5-116) will form an engineer task force to build these defense and Army engineer units will constitute the majority of forces available to construct them. These Army engineer organizations can be assisted by Navy construction battalions, Air Force engineers, and a wide variety of civilian construction companies. The CINC's, joint-force commander's, and ASCC's ability to influence the battle with engineer assets may be managed through operating a theater contingency engineering management (TCEM) or a regional contingency engineering management (RCEM) cell. The respective geographic CINCs govern the composition and the procedures of the TCEM and the RCEM cells. These cells augment the staffs they support and do not form an engineer-command stovepipe. The TCEM and the RCEM cells apply the commander's intent, merge engineer-support requirements, and orchestrate resources by—

- Establishing priorities and policy for theater Class IV (A and B) stockage levels.
- Establishing theater distribution protocols that are consistent with construction priorities.
- Monitoring and recommending the allocation and use of construction assets against priority operational requirements and recommending taskings for engineer assets.
- Developing construction standards and priorities.
- Providing input to the Joint Civil-Military Engineering Board (JCMEB).[110]

CONTROL MEASURES

The basic graphic control measures associated with offensive and defensive operations found in FM 3-90 also apply to the development of operationally significant defenses. The operational commander will give units charged with the construction of operationally significant defenses an area of operations and control the development of obstacles using obstacle control measures, to include designation of obstacle zones, belts, and groups, and any restrictions appropriate to the situation.

PLANNING

Defensive operations defeat an enemy attack, buy time, economize forces, or develop conditions favorable for offensive operations. Defensive operations alone normally cannot achieve a decision. Their purpose is to create conditions for a counteroffensive that allows Army forces to regain the initiative.[111] Other reasons for conducting defensive operations include—

- Retaining decisive terrain or denying a vital area to the enemy.
- Attritting or fixing the enemy as a prelude to offensive operations.
- Surprise action by the enemy.
- Increasing the enemy's vulnerability by forcing him to concentrate his forces.[112]

The planning considerations associated with tactical area and mobile defenses laid out in Chapters 9 and 10 of FM 3-90 also apply to the creation of an operationally significant defense. Significant operational level defenses typically take advantage of significant linear obstacles, such as mountain ranges, major rivers, and urban areas perpendicular to potential enemy lines of operation, to increase their effectiveness. The commander's keys to a successful tactical defense are applicable at the operational level—

- Capability to concentrate effects.
- Depth of the defensive area.
- Security.
- Ability to take full advantage of the terrain.
- Flexibility of defensive operations.
- Timely resumption of offensive operations.[113]

Creation of operationally significant defenses requires the expenditure of significant resources in terms of time as well as units and supplies devoted to the construction effort. The planning effort associated with such defenses account for these factors.

Operationally significant defenses provide cover and mitigate the effects of enemy weapons. Engineers may be called on to mass their skills and equipment, augmenting combat units in developing defensive positions into fortifications or strongpoints and in improving defensive positions. More often, however, engineers participate in and provide staff advice on camouflage, concealment, and deception (CCD) measures and the hardening of facilities to resist the destruction of C2 facilities (as part of integrated plans), air-defense weapons systems, and support structures. (See FMs 3-34 (5-100), 3-34.112 (5-103), and 5-114 (which will be consolidated into the next edition of FM 3-34) for more information on techniques and procedures for survivability and force protection.)[114]

An operational commander directing the creation of such defenses must be sure that the benefits gained will be worth the effort. Historically asymmetric means often negate such de-

fenses. The German attack through the Ardennes in May 1940 bypassed the main part of the Maginot Line. The Manchus were allowed through the great wall during the mid 17th Century when they were invited to help put down a peasant revolt. Plans for operations that take advantage of these defenses take into account asymmetric attacks designed to reduce their effectiveness.

PREPARING

Preparations focus on those intelligence, surveillance, and reconnaissance operations required to answer the commander's critical information requirements, refining the defensive plan, increasing coordination and synchronization, and conducting shaping actions within the force's capability and operations security guidelines. If the commander decides that he must conduct a deliberate defense but knows that the enemy will attack before he is prepared, he may have to commit substantial forces to security operations or conduct a spoiling attack. This buys time and space to further prepare for the conduct of a deliberate defense. Those area defense preparation considerations outlined in Chapter 9 of FM 3-90 also apply at the operational level.[115]

EXECUTING

An operational commander using operationally significant defenses will use a variety of tactics, techniques, and procedures to accomplish his mission. At one end of his options is a totally static defense oriented on terrain retention. This defense depends on the use of firepower from fixed positions to deny the enemy terrain. At the other end is a dynamic defense focused on the enemy. That defense depends on maneuver to disrupt and destroy the enemy force.[116] The tactical area defense execution considerations outlined in Chapter 9 also apply to the defense of an operationally significant defense.

REMOVAL OF OPERATIONALLY SIGNIFICANT HAZARDS

The operational commander eliminates or reduces operationally significant hazards that adversely affects execution of his plan. Alternatively, the removal of operationally significant hazards, such as undocumented minefields and toxic chemicals, may be a major objective within the context of a stability operation. Removal of operationally significant hazards allows maneuver during the conduct of offensive and defensive operations despite the presence of isolated obstacles. Alternatively, in stability or support operations it allows the civilian population located within the area of operations to resume their normal activities.

While obstacle breaching is a synchronized combined-arms operation under the control of a maneuver commander, hazard removal is normally an engineer or contractor operation under

the control of the force engineer. Other US governmental or host nation agencies, such as the Environmental Protection Agency (EPA) or the Federal Emergency Management Agency (FEMA), may be the lead agency and be in charge of the hazard removal effort depending on the type of hazard present and the factors of METT-TC. Nevertheless, there are many similarities between breaching operations and hazard removal operations.

Breaching operations begin when friendly forces detect an obstacle and begin to apply the breaching fundamentals, and they end when battle handover has occurred between follow-on forces and a unit conducting the breaching operation. Hazard removal likewise begins when friendly forces detect the hazard, but may not end until the hazard is reduced or neutralized and no longer posses a threat to the civilian population of an area.[117]

ORGANIZATION OF FORCES

A commander organizes friendly forces to accomplish the breaching fundamentals quickly and effectively. This requires him to organize support, breach, and assault forces with the necessary assets to accomplish their roles

CONTROL MEASURES

The FM 3-34.2 (90-13-1) control measures associated with obstacle breaching also apply to the removal of operationally significant hazards. In some cases, definitions need modification to enable them to remain relevant to hazard removal. The following modified definitions apply to hazard removal:

- Hazard. A hazard is any environmental factor that disrupts, fixes, turns, or blocks the movement of animals, vehicles, or personnel while simultaneously threatens the physical integrity or health of equipment, animals, or people in its vicinity. Hazards can also negatively affect plant life and threaten the environment within an AO. Hazards can exist naturally, be man-made (reinforcing), or be a combination of both.[118]
- Reduce. This is a tactical mission task to create and mark lanes through, over, or around a hazard that allow friendly forces to accomplish their mission and supported civil populations to continue their economic lives.[119]
- Clearing. This is the total elimination or neutralization of a hazard or a portion of a hazard at a given location.[120]

Planning

Units develop plans to conduct a breaching operation using the military decision-making process (MDMP). For a complete discussion of the MDMP, see FM 5-0 (101-5). Chapter 2 of FM 3-34.2 (90-13-1) deals specifically with the MDMP during the conduct of combined arms breach operations.

The scheme of maneuver, engineer operations, fires, air defense, and actions at obstacles are based on the same situational template. Planners develop the plan for removing operationally significant hazards using the following sequence:

- Reverse planning begins with what actions within the area need to be restored to accomplish the mission.
- Actions on the objective drive the size and composition of the assault force.
- The size of the assault force determines the number and location of lanes to be created.
- Lane requirements and the type of obstacle drive the amount and type of mobility assets task-organized to the breach force.
- The ability of the enemy to interfere with the reduction of the obstacle determines the size and composition of the security element in the breach force.
- The ability of the enemy to mass fires on the point of breach determines the amount of suppression required and the size and composition of the support force.

Preparing

The breaching tenets in FM 3-34.2 (90-13-1) apply with slight modifications to the removal of operationally significant hazards. These tenets should be applied whenever a hazard is encountered in the AO. The tenets are—

- Intelligence.
- Breaching fundamentals.
- Breaching organization.
- Mass.
- Synchronization.

See FM 3-34.2 (90-13-1) for a detailed discussion of each breaching tenet.[121]

The operational commander's G3, G2, Medical Officer, and ENCOORD direct hazard intelligence collection efforts within their areas of staff responsibilities to ensure the detection, recording, and analysis of every significant hazard within the area of operation. This includes determination of the specific characteristics of each hazard encountered. Examples of information needed to fill hazard information requirements are found in FM 3-34.2 (90-13-1).

Obtaining hazard intelligence information requires dedicated collection assets. These assets identify survivability positions and obstacle emplacement activity. Aviation units, ground cavalry, military police, chemical and biological reconnaissance elements tasked to perform reconnaissance in the area, may be able to provide valuable information by visual information or by the use of available sensors.[122]

Units and individuals removing hazards from an area of operations need specialized training to enable them to respond correctly to the wide range of hazards found within the area of operations. Hazards resulting from the employment of normal military obstacles are fully docu-

mented in mission training plans and individual soldier books. Asymmetric hazards resulting from chemical, biological, or radiological hazards require specialized training and equipment to counteract. Operational commanders and their staffs must be innovative in preparing how they and their forces will respond to these asymmetric hazards. Host nation or third nation forces and civilians may also need training in the identification, locating, and safe disposal of hazardous materiel, such as mines and unexploded ordnance.

Executing

An operational commander seeking to remove operationally significant hazards from his area of operation employs the breaching fundamentals—suppress, obscure, secure, reduce, and assault (SOSRA) described in detail in FM 3-34.2 (90-13-1). These fundamentals will always apply, but their application will vary based on the specific factors of METT-TC applicable to each specific assigned task.[123]

CONCLUSION

Doctrine provides a common philosophy to those military organizations affected by it. It defines the common language that military professionals use to provide and understand the commander's intent and ensure unity of effort. This research project provided a draft doctrinal operational force protection chapter that could quickly be adapted for use in a future Army large unit operations field manual. The Army echelons that normally conduct large unit operations are corps or numbered army headquarters operating as the Army Force (ARFOR), joint force land component command (JFLCC), or a joint task force headquarters. The Army service component command assigned to each commander of a combatant command also operates at the operational and theater strategic levels.

The five components of force protection defined in FM 3-0 (100-5), *Operations*, provided the basic structure of this research project—air, space, and missile defense; nuclear, biological, and chemical defense; antiterrorism; defensive information operations; and security to operational forces and means. The research project takes as a given the theater level structure documented in joint publications and the current draft FM 3-93 (100-7), with the exception that it assumes that the deputy commander of the Army operational-level echelon is the JRAC called for by joint doctrine but never designated. Operational force protection represents a critical capability for the joint force commander. Mission accomplishment cannot result solely from the conduct of operational force protection, but mission failure could well be a result of failures in the provision of operational force protection. Therefore, it is important that all operational-level commanders—combat, combat support, and combat service support—consider the threats to

their units and train them to the challenges provided by enemies conducting symmetrical and asymmetrical operations against their command.

This research project did not address some activities associated with the JP 1-02 definition of force protection because CJCSM 3500.04B, *Universal Joint Task List*, groups them with other related theater strategic and operational level tasks. These activities include—

- Individual health and welfare activities.
- Dispersion and mobility actions.
- Offensive counter air activities.
- Defensive IO actions comprising actions taken to maintain the integrity of friendly information despite adversary offensive IO.

In an attempt to reduce unnecessary duplication, this draft chapter also made extensive references to other joint publications (JPs) and field manuals (FMs).

Word count = 17,681

ENDNOTES

[1] Department of Defense, *Department of Defense Dictionary of Military and Associated Terms,* Joint Pub 1-02, (Washington, D.C.: U.S. Department of Defense), 182.

[2] Department of the Army, *Operations*, Field Manual (FM) 3-0 (100-5), (Washington, D.C.: U.S. Department of Defense,14 June 2001), 4-8.

[3] Department of Defense, *Joint Universal Task List,* Chairman, Joint Chiefs of Staff Manual (CJCSM) 3500.04B, (Suffolk, VA: Department of Defense, 1 November 1999), 1-3.

[4] Department of the Army, *Joint Air Operations Center and Army Air and Missile Defense Command Coordination,* FM 3-01.20 (new manual), (Washington, D.C.: US Department of Defense, January 2001), 1-4.

[5] Department of the Army, *Army Theater Missile Defense Operations,* FM 3-01.12 (100-12), (Washington, D.C.: US Department of Defense, 31 March 2000), 3-3 to 3-5.

[6] Department of the Army, *Army Air and Missile Defense Command Operations*, FM 3-01.94 (44-94), (Washington, D.C.: US Department of Defense, 31 March 2000), 2-3.

[7] Ibid, B-3.

[8] Department of the Army, *U.S. Army Air and Missile Defense Operations*, FM 3-01 (44-100), (Washington, D.C.: US Department of Defense, 15 June 2000), 5-18 to 5-19.

[9] FM 3-01.94 (44-94), 3-5 to 3-6.

[10] Ibid, 3-9

[11] FM 3-01 (44-100), 4-7 to 4-8.

[12] Department of Defense, Joint Pub 3-01, *Joint Doctrine for Countering Air and Missile Threats*, (Washington, D.C.: US Department of Defense, 19 October 1999), 1-2.

[13] FM 3-01.94 (44-94), 3-10 to 3-11.

[14] Ibid, 3-12.

[15] Department of Defense, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical NBC Environments*, JP 3-11, (Washington, D.C.: US Department of Defense, 11 July 2000), II-5

[16] Ibid, I-6

[17] Ibid, III-4 to III-6

[18] Department of the Army, *Chemical Operations Principles and Fundamentals*, FM 3-11 (3-100), (Washington, D.C.: US Department of Defense, 8 May 1996), 4-1 to 4-10.

[19] Department of the Army, *The Army in Theater Operations*, Second Draft, FM 3-93 (100-7), (Carlisle Barracks, PA: US Department of Defense, March 2001), 9-50 to 9-51.

[20] Ibid, 9-52.

[21] Ibid, 9-48 to 9-49.

[22] FM 3-11 (3-100), 7-0 to 7-9.

[23] FM 3-93 (100-7), 9-44.

[24] Ibid.

[25] Ibid, 9-44 to 9-45.

[26] Ibid, 9-45.

[27] Department of the Army, *Multiservice Procedures for Nuclear, Biological, and Chemical Protection of Fixed Sites*, FM 3-11.34 (3-4-1), (Washington, D.C.: US Department of Defense, September 2000), III-1 to III-3.

[28] Ibid, III-3.

[29] Ibid.

[30] Ibid, III-4.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Ibid, III-5.

[36] FM 3-93 (100-7), 9-45.

[37] Ibid, 9-45 to 9-46.

[38] Ibid, 9-46.

[39] Ibid.

[40] Ibid, 9-46 to 9-47.

[41] Ibid, 9-47.

[42] Ibid.

[43] Ibid, 9-52.

[44] Ibid, 9-52 to 9-53.

[45] Ibid, 9-53 to 9-54.

[46] FM 3-11.34 (3-4-1), I-1.

[47] *Joint Tactics, Techniques, and Procedures for Antiterrorism*, Joint Pub 3-07.2, (Washington, D.C.: US Department of Defense, 17 March 1998), vii to viii.

[48] Ibid, viii.

[49] Joint Pub 1-02, 35.

[50] *Joint Doctrine for Military Operations Other Than War*, Joint Pub 3-07, (Washington, D.C.: US Department of Defense, 16 June 1995), III-2.

[51] *Joint Tactics, Techniques, and Procedures for Antiterrorism*, Joint Pub 3-07.2, (Washington, D.C.: US Department of Defense, 17 March 1998), ix.

[52] Ibid.

[53] Ibid, II-10.

[54] Ibid, II-11.

[55] Ibid, IV-7.

[56] Ibid, IV-9 to IV-10.

[57] Ibid, IV-1 to IV-2.

[58] Ibid, VII-1 to VII-2.

[59] Ibid, VII-2.

[60] Ibid, IV-9.

[61] Ibid, VI-2.

[62] Ibid, VI-3.

[63] Ibid.

[64] Ibid.

[65] Department of the Army, *Information Operations: Doctrine, Tactics, Techniques, and Procedures*, Final Draft FM 3-13 (100-6), (Leavenworth, KS: US Department of Defense, 30 Sep 2000), 1-11 to 1-12.

[66] Ibid, 1-14.

[67] *Joint Doctrine for Information Operations*, JP 3-13, (Washington, D.C.: US Department of Defense, 9 October 1998), III-1.

[68] Final Draft FM 3-13 (100-6), 1-15 to 1-16.

[69] JP 3-13, IV-1.

[70] Final Draft FM 3-13 (100-6), F-7 to F-8.

[71] FM 3-93 (100-7), 7-6.

[72] Final Draft FM 3-13 (100-6), F-16 to F-18.

[73] Ibid, F-20.

[74] Ibid, 4-6.

[75] Ibid, 3-2.

[76] Ibid, 3-2 to 3-3.

[77] Ibid, 3-3.

[78] Ibid.

[79] Ibid.

[80] JP 3-13, III-8.

[81] Ibid., III-8 to III-9.

[82] Ibid, III-9.

[83] Ibid, III-9 to III-10.

[84] Ibid, III-10.

[85] Ibid.

[86] Ibid.

[87] Ibid.

[88] Ibid.

[89] Ibid.

[90] Ibid.

[91] Ibid, III-10 to III-11.

[92] Ibid, III-11.

[93] Ibid, III-11 to III-12.

[94] Ibid, III-12.

[95] Ibid.

[96] Ibid, III-12 to III-13.

[97] Ibid, III-13.

[98] Ibid.

[99] Ibid.

[100] Ibid.

[101] Ibid, III-14.

[102] Ibid.

[103] Ibid.

[104] Ibid.

[105] Ibid, III-14 to III-15.

[106] Ibid, III-15.

[107] Ibid.

[108] *Tactics*, FM 3-90, (Washington, D.C.: US Department of Defense, 4 July 2001), 12-0 to 12-1.

[109] Department of the Army, *Engineer Operations: Echelons Above Corps*, FM 3-34.211 (5-116), (Washington, D.C.: US Department of Defense, 5 Feb 99), 5-2.

[110] Ibid, 2-5.

[111] FM 3-0 (100-5), 1-15.

[112] FM 3-90, 8-1 to 8-2.

[113] Ibid, 9-7.

[114] FM 3-34.211 (5-116), 1-6 to 1-7.

[115] FM 3-90, 9-13.

[116] Ibid, 9-16.

[117] Department of the Army, *Combined Arms Breaching Operations*, with Change #2, FM 3-34.2 (90-13-1), (Washington, D.C.: US Department of Defense, 26 Feb 2001), 1-1.

[118] Ibid.

[119] FM 3-34.2 (90-13-1), 1-2.

[120] Ibid.

[121] Ibid, 1-4.

[122] Ibid, 1-5.

[123] Ibid, 1-6.

BIBLIOGRAPHY

Chairman of the Joint Chiefs of Staff Manuals

U.S. Department of Defense. *Universal Joint Task List.* Chairman of the Joint Chiefs of Staff Manual 3500.04B. Suffolk, VA: U.S. Department of Defense,1 November 1999.

Joint Publications

U.S. Department of Defense. *Unified Action Armed Forces (UNAAF).* Joint Publication 0-2. Washington, D.C.: U.S. Department of Defense, 24 February 1995.

U.S. Department of Defense. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication 1-02. Washington, D.C.: U.S. Department of Defense, 1 September 2000.

U.S. Department of Defense. *Joint Intelligence Support to Military Operations.* Joint Publication 2-01. Washington, D.C.: U.S. Department of Defense, 20 November 1996.

U.S. Department of Defense. *Doctrine for Joint Operations.* Joint Publication 3-0. Washington, D.C.: U.S. Department of Defense, 1 February 1995.

U.S. Department of Defense. *Joint Doctrine for Countering Air and Missile Threats.* Joint Publication 3-01. Washington, D.C.: U.S. Department of Defense, 19 October 1999.

U.S. Department of Defense. *Doctrine for Joint Theater Missile Defense.* Joint Publication 3-01.5. Washington, D.C.: U.S. Department of Defense, 22 February 1996.

U.S. Department of Defense. *Joint Doctrine for Military Operations Other Than War.* Joint Publication 3-07. Washington, D.C.: U.S. Department of Defense, 16 June 1995.

U.S. Department of Defense. *Joint Tactics, Techniques, and Procedures for Antiterrorism.* Joint Publication 3-07.2. Washington, D.C.: U.S. Department of Defense, 17 March 1998.

U.S. Department of Defense. *Doctrine for Joint Fire Support.* Joint Publication 3-09. Washington, D.C.: U.S. Department of Defense, 12 May 1998.

U.S. Department of Defense. *Doctrine for Joint Rear Area Operations*, Joint Publication 3-10. Washington, D.C.: U.S. Department of Defense, 28 May 1996.

U.S. Department of Defense. *Joint Tactics, Techniques, and Procedures for Base Defense.* Joint Publication 3-10.1. Washington, D.C.: U.S. Department of Defense, 23 July 1996.

U.S. Department of Defense. *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments.* Joint Publication 3-11. Washington, D.C.: U.S. Department of Defense, 11 July 2000.

U.S. Department of Defense. *Joint Force Capabilities.* Joint Publication 3-33. Washington, D.C.: U.S. Department of Defense, 13 October 1999.

U.S. Department of Defense. *Doctrine for Joint Airspace Control in a Combat Zone.* Joint Publication 3-52. Washington, D.C.: U.S. Department of Defense, 22 July 1995.

U.S. Department of Defense. *Doctrine for Health Service Support in Joint Operations.* Joint Publication 4-02. Washington, D.C.: U.S. Department of Defense, 26 April 1995.

U.S. Department of Defense. *Joint Doctrine for Civil Engineering Support.* Joint Publication 4-04. Washington, D.C.: U.S. Department of Defense, 26 September 1995.

Army Publications

U.S. Department of the Army. *Intelligence Preparation of the Battlefield.* Field Manual 2-01.3 (34-130) . Washington, D.C.: U.S. Department of Defense, 8 July 1994.

U.S. Department of the Army. *Operations.* Field Manual 3-0. Washington, D.C.: U.S. Department of Defense, 14 June 2001.

U.S. Department of the Army. *Army Theater Missile Defense Operations.* Field Manual 3-01.12 (100-12) . Washington, D.C.: U.S. Department of Defense, 31 March 2000.

U.S. Department of the Army. *Chemical Operations Principles and Fundamentals.* Field Manual 3-11 (3-100) . Washington, D.C.: U.S. Department of Defense, 8 May 1996.

U.S. Department of the Army. *Chemical & Biological Contamination Avoidance.* Change 1 to Field Manual 3-11.3 (3-3). Washington, D.C.: U.S. Department of Defense, 29 September 1994.

U.S. Department of the Army. *NBC Protection.* Field Manual 3-11.4 (3-4). Washington, D.C.: U.S. Department of Defense, 29 May 1992.

U.S. Department of the Army. *Multiservice Tactics, Techniques, and Procedures for NBC Defense of Theater Fixed Sites, Ports, and Airfields.* Field Manual 3-11.34 (3-4-1). Washington, D.C.: U.S. Department of Defense, 29 September 2000.

U.S. Department of the Army. *Biological Defense Operations Corps/Company Tactics, Techniques, and Procedures.* Change 1 to Field Manual 3-11.86 (3-101-6). Washington, D.C.: U.S. Department of Defense, 1 September 2000.

U.S. Department of the Army. *Information Operations (Final Draft).* Field Manual 3-13 (100-6). Washington, D.C.: U.S. Department of Defense, 30 September 2000.

U.S. Department of the Army. *Engineer Operations.* Field Manual 3-34 (5-100). Washington, D.C.: U.S. Department of Defense, 27 February 1996.

U.S. Department of the Army. *Combined Arms Breaching Operations.* Change 2 to Field Manual 3-34.2 (90-13-1). Washington, D.C.: U.S. Department of Defense, 23 Feb 2001.

U.S. Department of the Army. *Army Airspace Command and Control* (DRAG Edition). Field Manual 3-52 (100-103). Washington, D.C.: U.S. Department of Defense, 4 July 2001.

U.S. Department of the Army. *Tactics, Techniques, and Procedures for the Targeting Process.* Field Manual 3-60 (6-20-10). Washington, D.C.: U.S. Department of Defense, 8 May 1996.

U.S. Department of the Army. *Tactics.* Field Manual 3-90. Washington, D.C.: U.S. Department of Defense, 4 July 2001.

U.S. Department of the Army. *Environmental Considerations in Military Operations.* Change 1 to Field Manual 3-100.4 (20-400). Washington, D.C.: U.S. Department of Defense, 11 May 2001.

U.S. Department of the Army. *Multiservice Procedures for Unexploded Ordnance Operations.* Field Manual 3-100.38 (100-38). Washington, D.C.: U.S. Department of Defense, 23 August 2001.

U.S. Department of the Army. *Preventative Medicine Services.* Field Manual 4-02.17 (8-10-17). Washington, D.C.: U.S. Department of Defense, 28 August 2001.

U.S. Department of the Army. *Army Planning and Orders Production (Initial Draft).* Field Manual 5-0 (101-5) . Leavenworth, KS: U.S. Department of Defense, 01 August 2001

U.S. Department of the Army. *Survivability.* Field Manual 3-34.112 (5-103) Washington, D.C.: U.S. Department of Defense, 10 June 1985.

U.S. Department of the Army. *Engineer Operations Short of War.* Field Manual 3-34 (5-114 incorporated into the current manual). Washington, D.C.: U.S. Department of Defense, 13 July 1992.

U.S. Department of the Army. *Engineer Operations: Echelon Above Corps.* Field Manual 3-34.211(5-116). Washington, D.C.: U.S. Department of Defense, 9 February 1999.

U.S. Department of the Army. *Health Service Support in a Theater of Operations.* Field Manual 4-02 (8-10). Washington, D.C.: U.S. Department of Defense, 1 March 1991.